Podstawy kryptografii
Wykład nr 1
Temat: Wprowadzenie do kryptografii

dr Michał Dolecki
Katedra Inteligencji Obliczeniowej
Zakład Uczenia Maszynowego

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

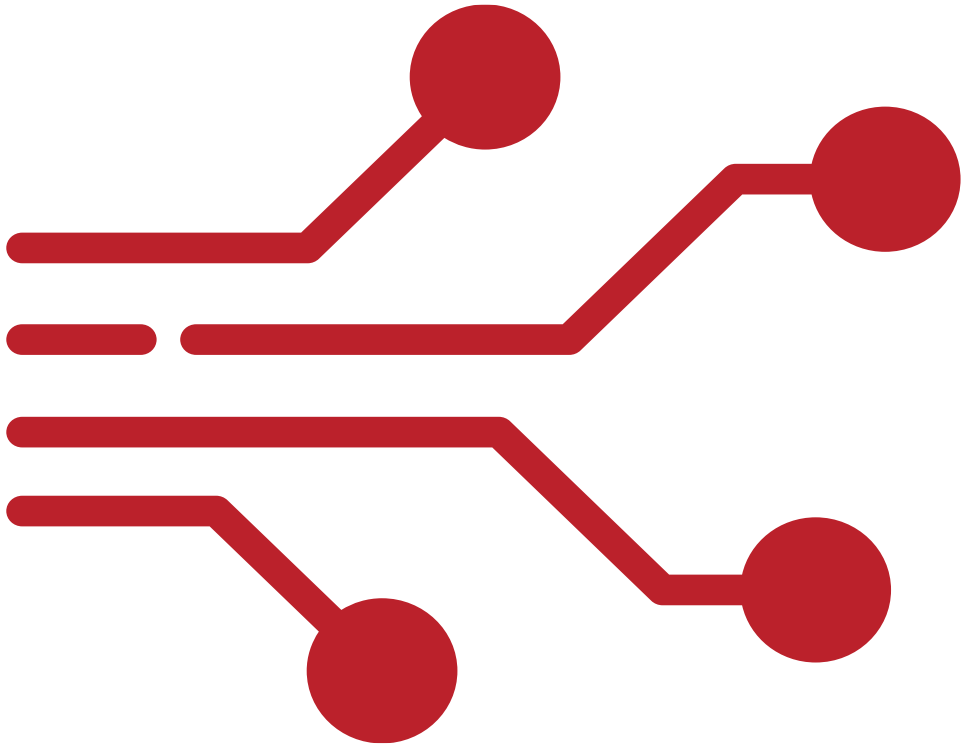
Plan wykładu

- Kryptografia jako nauka
- Podstawowe pojęcia
- Historia kryptografii

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

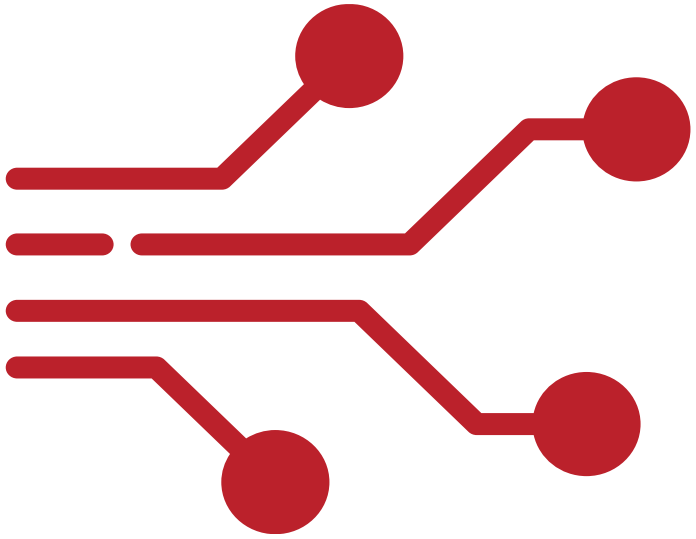
Kryptografia



Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

3

Kryptologia i jej dziedziny



Kryptologia

gr. *kryptós* 'ukryty', *lógos* 'słowo'

nauka o szyfrowaniu, tzn. o bezpiecznych sposobach przekazywania informacji

Kryptografia

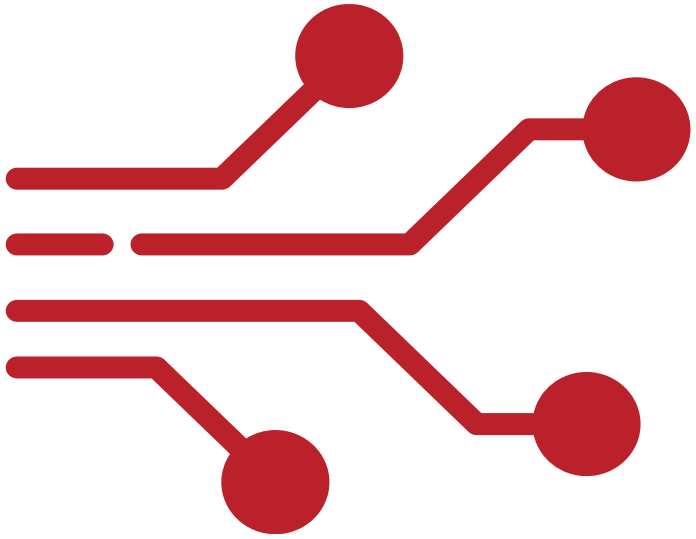
gr. *kryptós* 'ukryty', *gráphō* 'piszę'

ogół metod utajniania informacji za pomocą szyfrowania; dziedzina kryptologii

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

4

Kryptologia i jej dziedziny



Kryptoanaliza

gr. *kryptós* 'ukryty', *analýein* 'analizować'

nauka i sztuka rozszyfrowywania kryptosystemów w celu pozyskania informacji

Steganografia

gr. *steganos* 'ukryty, chroniony' i *graphein* 'pisać'

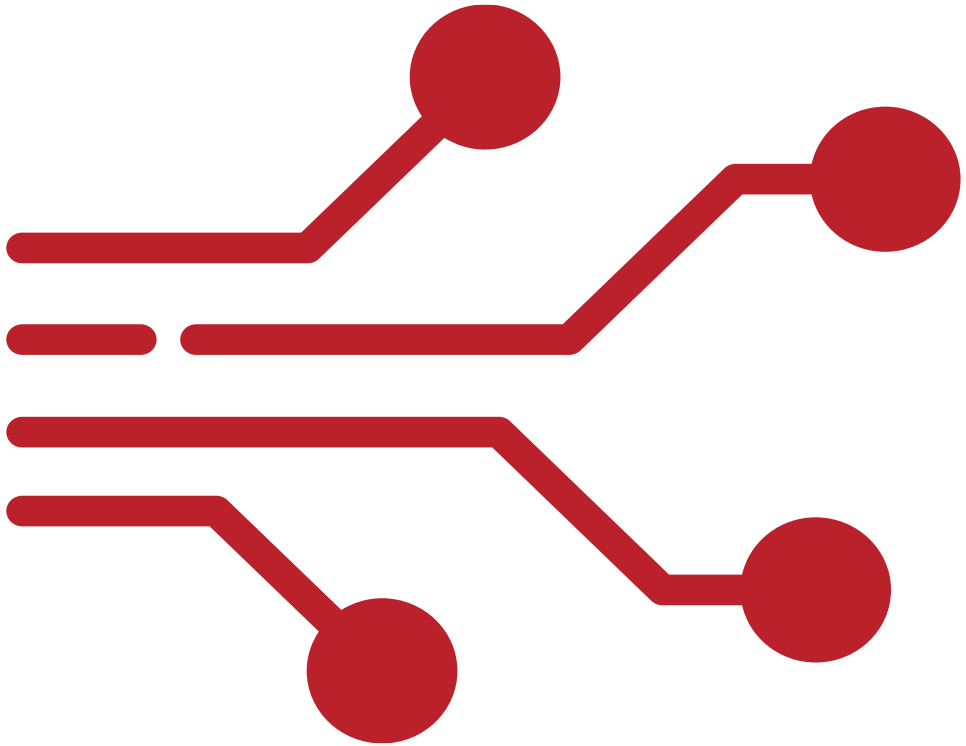
nauka o komunikacji w taki sposób, by obecność komunikatu nie mogła zostać wykryta

Źródła: Encyklopedia PWN, Słownik Języka Polskiego, Wikipedia

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

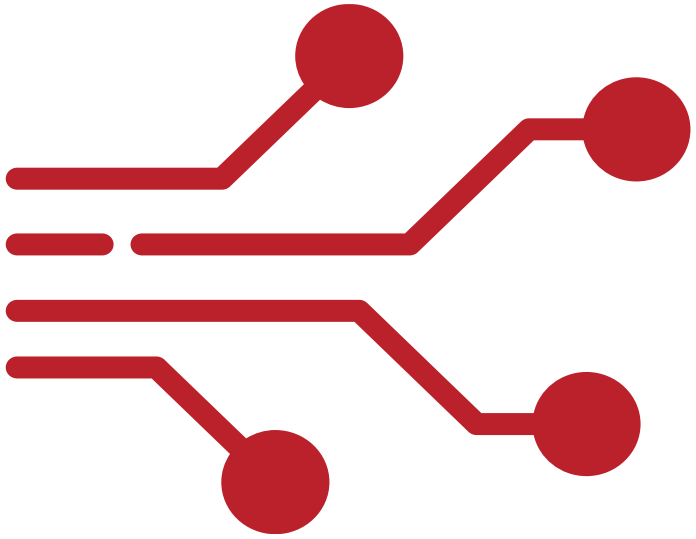
Podstawowe pojęcia



Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

6

Dane i informacje



Dana -- Informacja

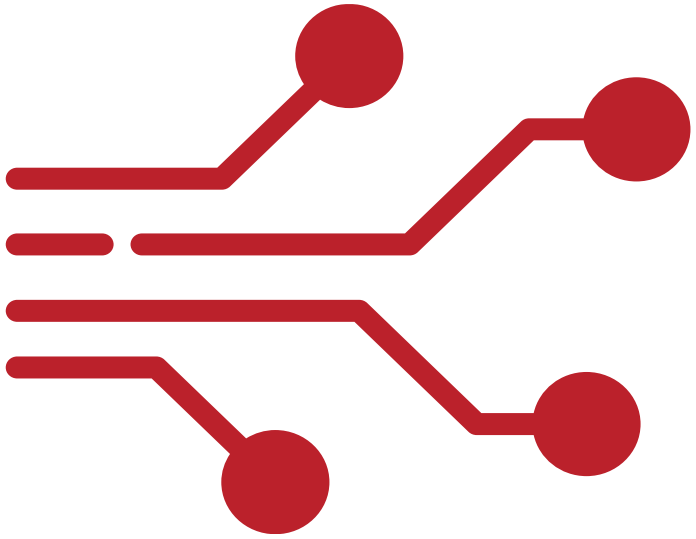
Ochrona danych -- ochrona informacji

Zrozumienie różnicy między daną a informacją oraz sposobów ich ochrony jest kluczowe dla każdego, kto zajmuje się bezpieczeństwem, ponieważ to, co chronimy, determinuje jak to chronimy.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

7

Pojęcie danej



Czym jest Dana? (Data)

To surowy, nieprzetworzony fakt, liczba, symbol lub obserwacja. Sama w sobie dana nie posiada znaczenia ani celu – jest po prostu cyfrowym lub fizycznym zapisem

Przykład: Liczba „39”, słowo „Kowalski”, ciąg bitów 10110

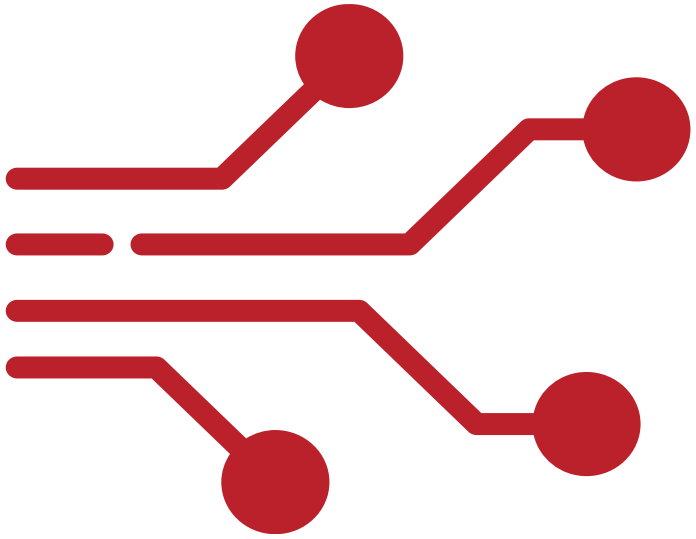
Są obiektywne, statyczne i nieprzetworzone

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

8

Pojęcie informacji



Czym jest Informacja? (Information)

Informacja powstaje, gdy danym nadamy kontekst, ustrukturyzujemy je i zinterpretujemy. Informacja odpowiada na pytania takie jak: *kto? co? gdzie? kiedy?*

Przykład: „Temperatura pacjenta wynosi 39°C” (liczba zyskała kontekst medyczny), „Jan Kowalski jest administratorem systemu”

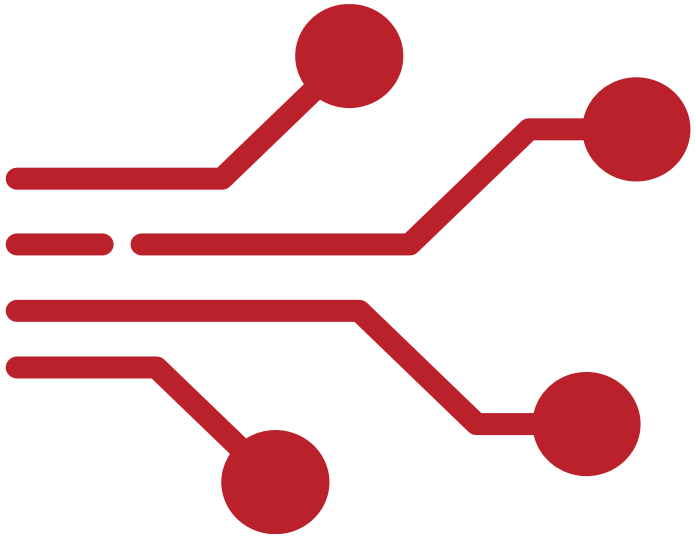
Jest subiektywna (zależy od odbiorcy) i celowa

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

9

Ochrona danych



Skupia się na technicznym i prawnym aspekcie zabezpieczenia samych rekordów

Główny cel: Zapewnienie, że dane nie zostaną utracone, uszkodzone i są przetwarzane zgodnie z prawem (np. RODO)

Zakres: Kopie zapasowe (backup), szyfrowanie dysków, retencja danych (jak długo je przechowujemy), ochrona danych osobowych

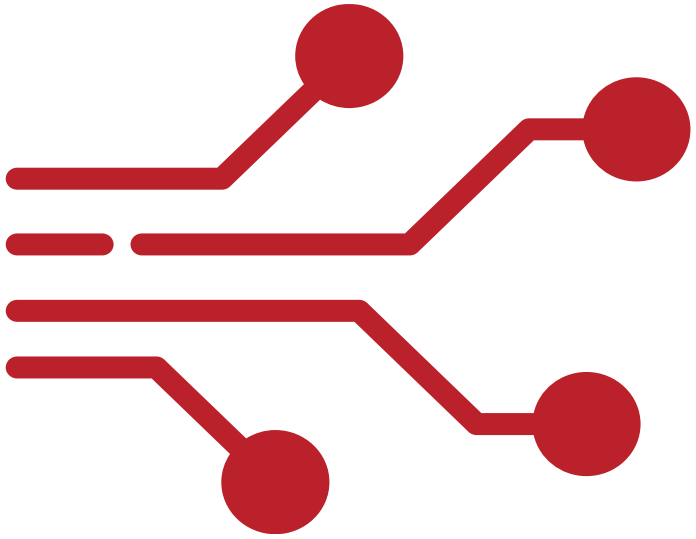
Pytanie: *Czy nasze bazy danych są bezpieczne i czy mamy prawo je posiadać?*

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

10

Ochrona informacji



Skupia się na wartości i znaczeniu treści. Jest pojęciem szerszym, obejmującym nie tylko bazy danych, ale i wiedzę w głowach pracowników czy tajemnice handlowe

Główny cel: Ochrona Triady CIA (Poufność, Integralność, Dostępność) w odniesieniu do aktywów informacyjnych firmy

Zakres: Klasyfikacja informacji (tajne, poufne), polityki czystego biurka, umowy NDA, zapobieganie wyciekom intelektualnym

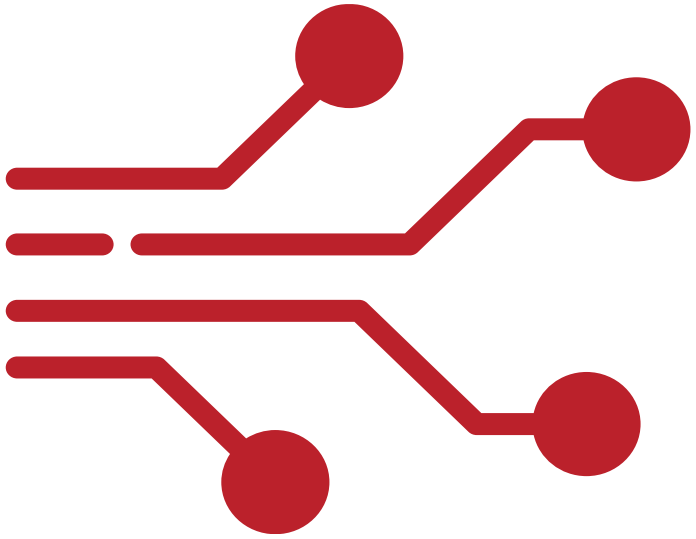
Pytanie: *Kto ma dostęp do naszej strategii biznesowej i czy jest ona autentyczna?*

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

11

Cele bezpieczeństwa (Triada CIA+)



Fundamentalne obszary zabezpieczania danych i informacji:

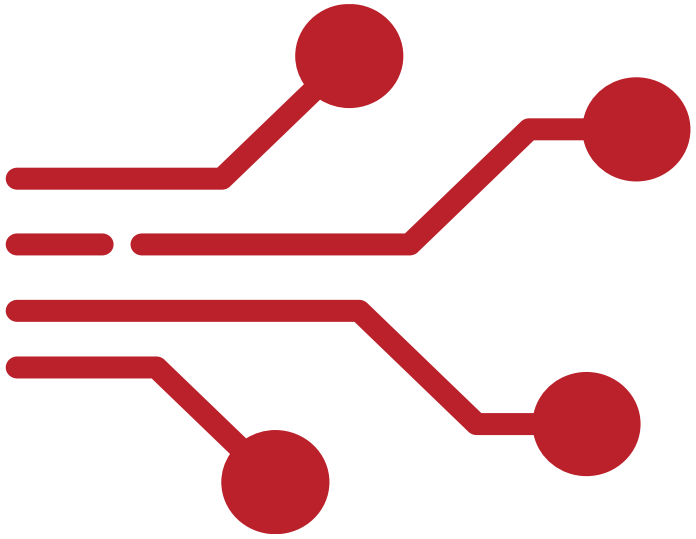
- Poufność (Confidentiality)
- Integralność (Integrity)
- Dostępność (Availability)
- Niezaprzeczalność (Non-repudiation)

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

12

Integralność



Sposoby zapewniania integralności danych:

- Kodowanie redundantne

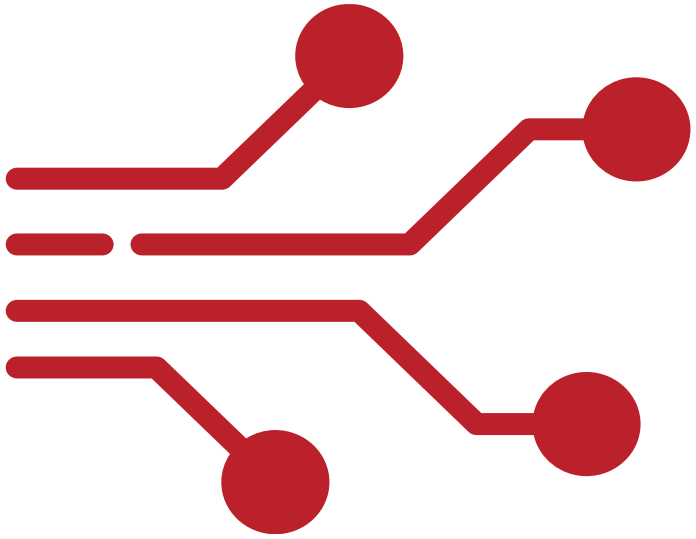
- Kody detekcyjne (EDC)
  - CRC
- Kody korekcyjne (ECC)
  - Kod Hamminga

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

13

Kod a szyfr



kody operują na znaczeniach/słowach

szyfry na poziomie bitów/znaków

kody nie ukrywają informacji, bo są znane jak kod binarny – każdy wie jak zapisać liczbę w systemie dwójkowym

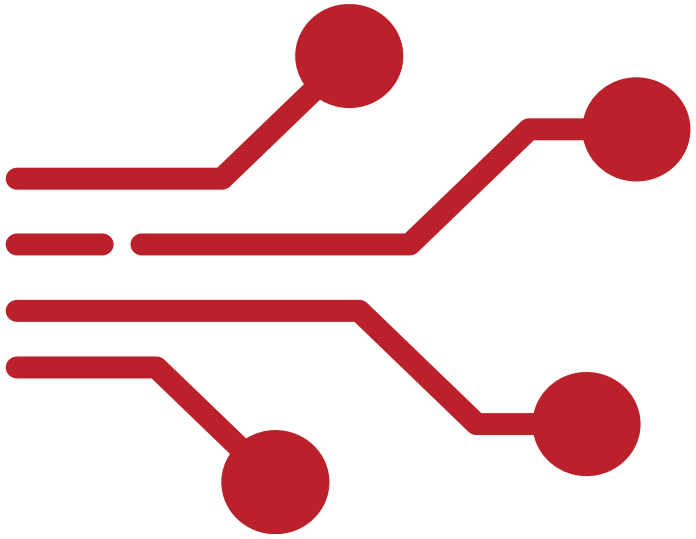
szyfry przekształcają informację w sposób czytelny tylko dla osób upoważnionych

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

14

Niezaprzeczalność i poufność



Niezaprzeczalność

Podpisy wiadomości (będą omawiane w dalszych wykładach)

Poufność informacji

Przekształcenie tekstu jawnego do szyfrogramu, który jest niezrozumiały dla nieuprawnionych stron komunikacji

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

15

Klasyczny podział kryptosystemów

- Kryptosystemy zamknięte
  (ang. *closed cryptographic systems*)
- Kryptosystemy otwarte
  (ang. *open cryptographic systems*)

historyczny podział kryptosystemów

obowiązywał przez wieki

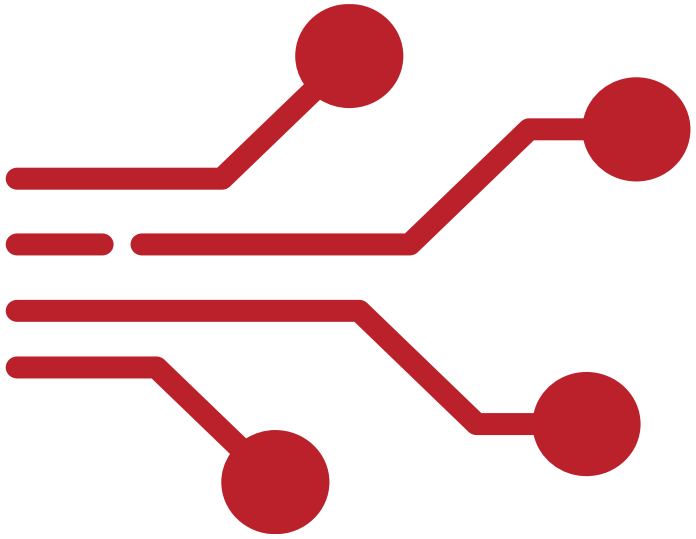
doskonale ilustruje ewolucję myślenia o bezpieczeństwie informacji.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

16

Kryptosystemy zamknięte



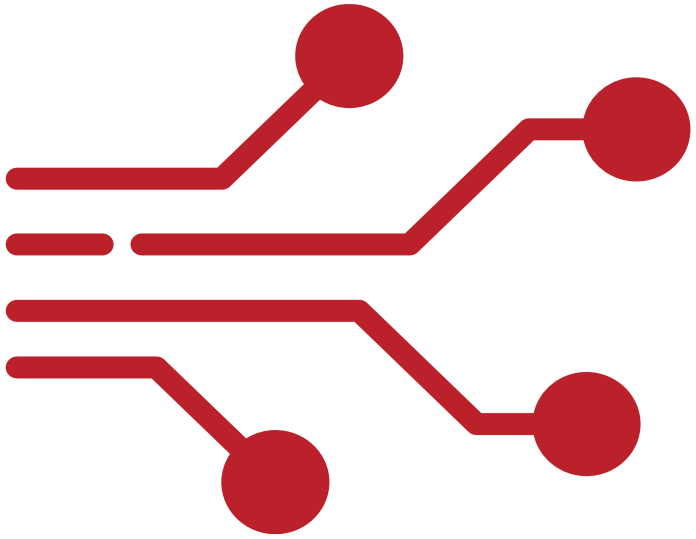
zarówno algorytm szyfrowania, jak i klucz (o ile w ogóle występował) stanowiły tajemnicę

bezpieczeństwo całego systemu opierało się na założeniu, że przeciwnik nie zna szczegółów działania zastosowanego szyfru

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

17

Zasada bezpieczeństwa



Podejście takie opiera się na zasadzie:

"Bezpieczeństwo przez niejasność"
ang. *security through obscurity*
innymi słowy
Skoro atakujący nie wie, jak działa szyfr,
nie będzie w stanie go złamać

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

18

Przykłady historyczne

Szyfry używane w starożytności i średniowieczu – często były to autorskie, nieudokumentowane metody, znane tylko wąskiemu gronu wtajemniczonych

Historia pokazała, że ta koncepcja jest głęboko wadliwa

Prędzej czy później algorytm trafiał w ręce wroga

Problem techniczny: jak szyfrować komunikację np. z bankiem dla tysięcy klientów?

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

19

Zasada Kerckhoffsa

jedna z podstawowych zasad współczesnej kryptografii

Auguste Kerckhoffs (1835 - 1903) – holenderski językoznawca i kryptograf, profesor języków

Artykuły *La Cryptographie Militaire* („Kryptografia wojskowa") 1883

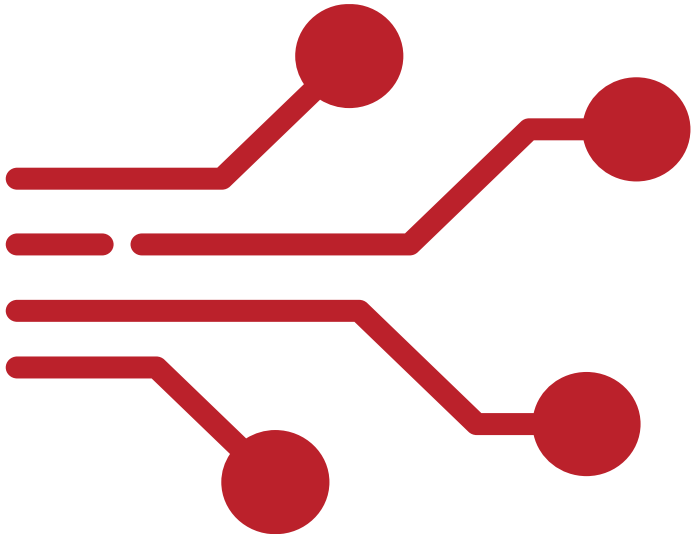
analizując ówczesne systemy kryptograficzne, sformułował sześć zasad, z których najsłynniejsza (druga) brzmi:

System nie powinien wymagać tajności, a wpadnięcie w ręce wroga nie powinno sprawiać kłopotu

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

20

Pełna lista zasad



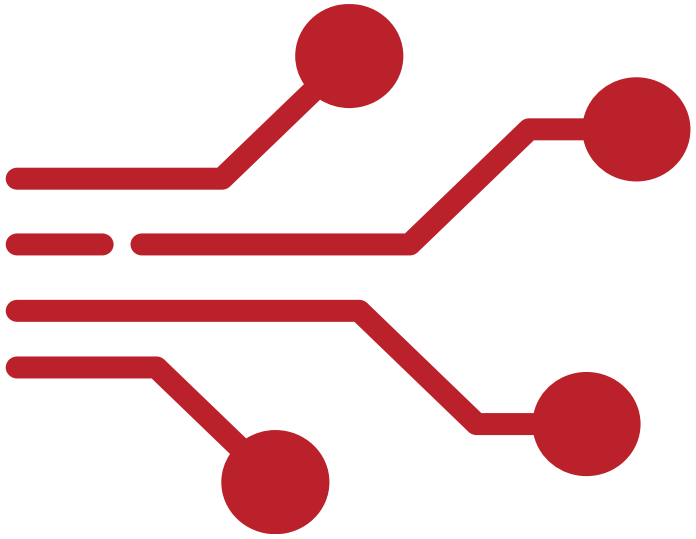
1. System powinien być, jeśli nie teoretycznie, to w praktyce nie do złamania.
2. **Projekt systemu nie powinien wymagać jego tajności, a ewentualne jego ujawnienie nie powinno przysparzać kłopotów korespondentom**
3. Klucz powinien być: możliwy do zapamiętania bez notowania i dodatkowo – łatwy do zmienienia.
4. Kryptogramy powinny być możliwe do przesłania drogą telegraficzną.
5. Aparatura i dokumenty powinny być możliwe do przeniesienia i obsłużenia przez jedną osobę.
6. System powinien być prosty – nie wymagający znajomości wielu reguł ani nie obciążający zbytnio umysłu.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

21

Kryptosystemy otwarte



algorytm szyfrowania jest jawny i powszechnie znany, natomiast tajemnicą jest wyłącznie klucz (parametr, który steruje działaniem algorytmu)

zakłada się, że *wróg* zna używany algorytm szyfrowania

bezpieczeństwo opiera się na tajności klucza

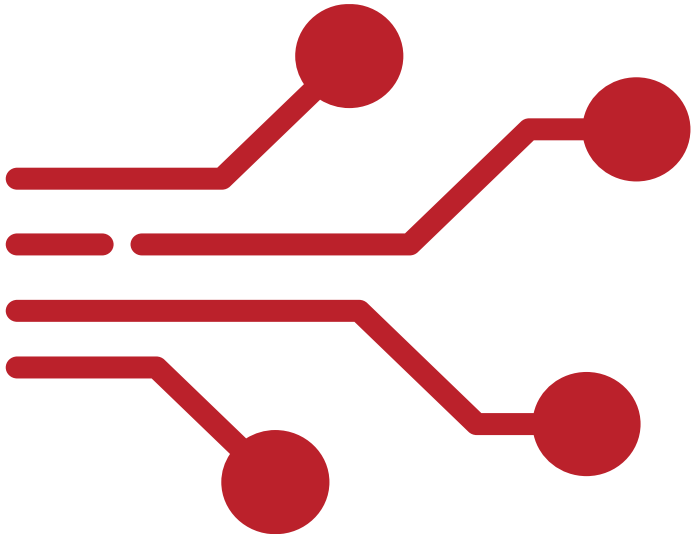
nawet jeśli atakujący zna dokładnie wszystkie szczegóły konstrukcji szyfru, nie jest w stanie odczytać wiadomości bez znajomości konkretnego klucza

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

22

Przykłady - AES



Przykłady już nie historyczne:

Algorytm AES (Advanced Encryption Standard)

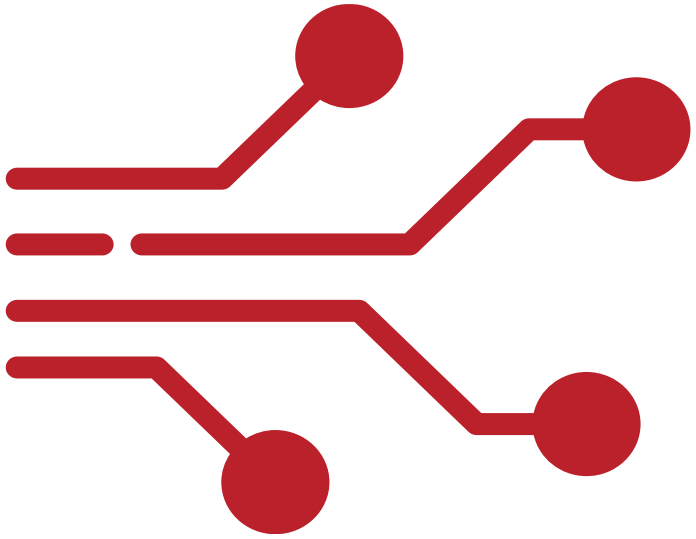
specyfikacja jest publicznie dostępna, a mimo to pozostaje bezpieczny, ponieważ klucz o odpowiedniej długości (np. 128, 192, 256 bitów) jest praktycznie niemożliwy do odgadnięcia.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

23

Przykłady – RSA, TLS



Algorytm RSA

opiera się na publicznie znanych zasadach matematycznych, ale bezpieczeństwo zapewnia trudność faktoryzacji dużych liczb, a klucz prywatny pozostaje tajny.

Protokół TLS (Transport Layer Security)

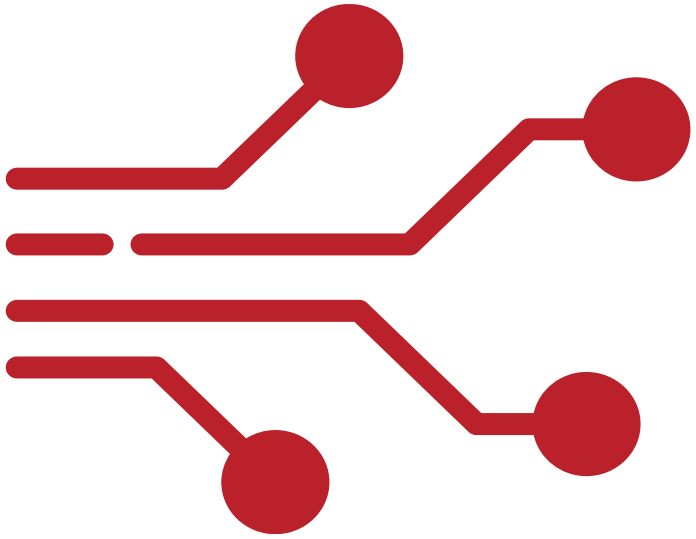
jego działanie jest dokładnie opisane w dokumentach RFC, a bezpieczeństwo zapewniają klucze sesji.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

24

Zalety kryptosystemów otwartych



Weryfikowalność: Jawny algorytm może być analizowany przez tysiące niezależnych ekspertów na całym świecie.

Standaryzacja: Otwarte algorytmy mogą stać się standardami (jak AES), co umożliwia ich implementację w różnych systemach i interoperacyjność.

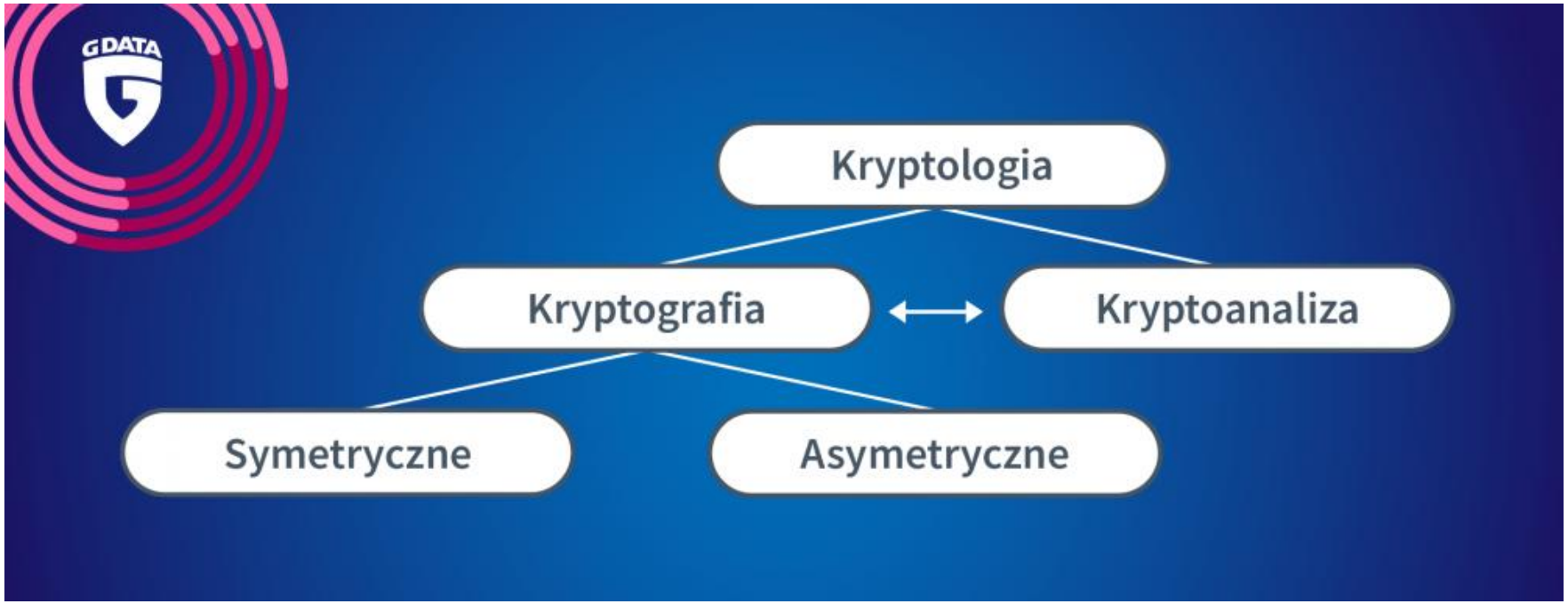
Bezpieczeństwo w dłuższej perspektywie: Nawet jeśli algorytm zostanie skompromitowany (np. odkryto w nim podatność), można go wymienić, nie ujawniając przeszłych wiadomości, o ile klucze pozostały tajne.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

25

Podział kryptologii



Źródło: https://gdata.pl/przewodnik/kryptografia

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

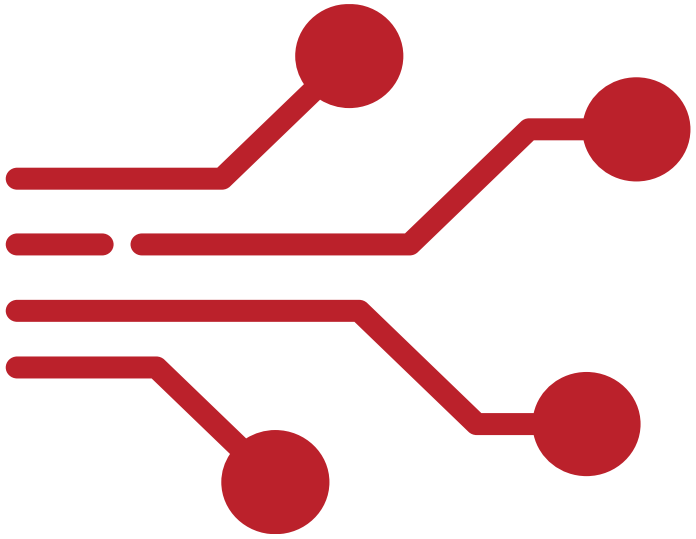
26

Historia kryptografii

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

27

Starożytny Egipt



umiejętność czytania hieroglifów jako sposób ukrywania informacji przed powszechnie niepiśmiennym ludem

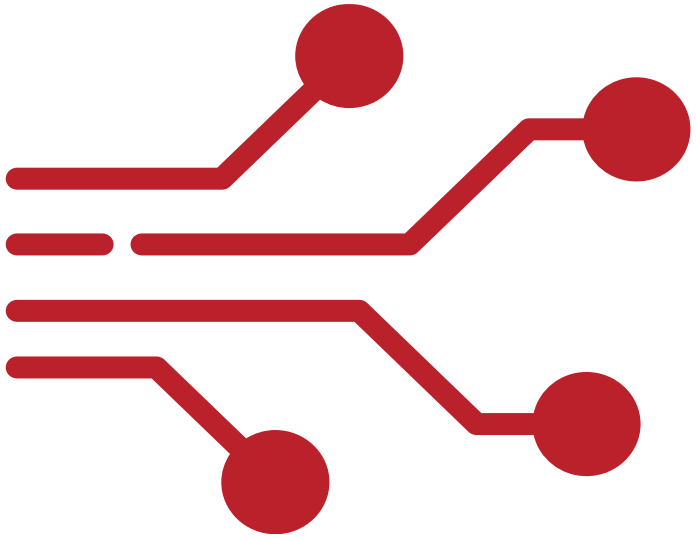
skrybowie używali też nietypowych hieroglifów. Nie miały one ukryć treści przed każdym, ale nadać inskrypcjom aurę tajemniczości i zmusić czytelnika do wysiłku intelektualnego

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

28

Mezopotamia



Pomijanie części znaków z tabliczek tocząc po nich rolki o określonym promieniu

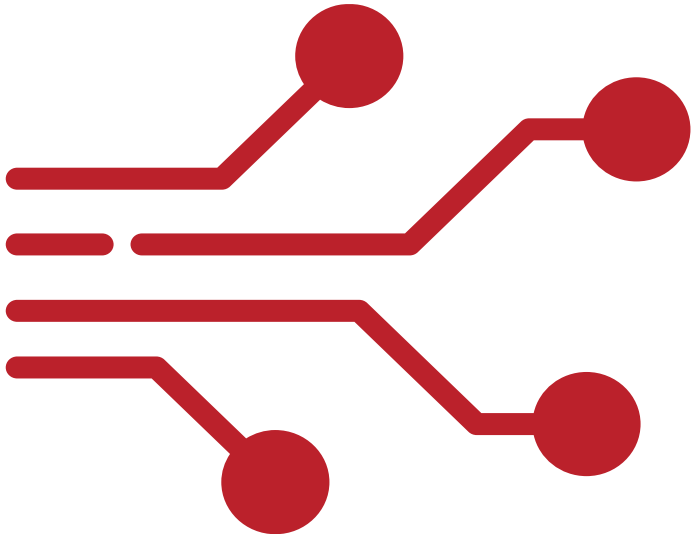
Podobne nieco do steganografii

Dla osoby nie znającej promienia rolki tekst mógł być po prostu losowymi znakami

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

29

Starożytna Grecja i Sparta



Spartanie używali urządzenia zwanego **Skytale**

drewniany wałek, na który nawijano pasek pergaminu

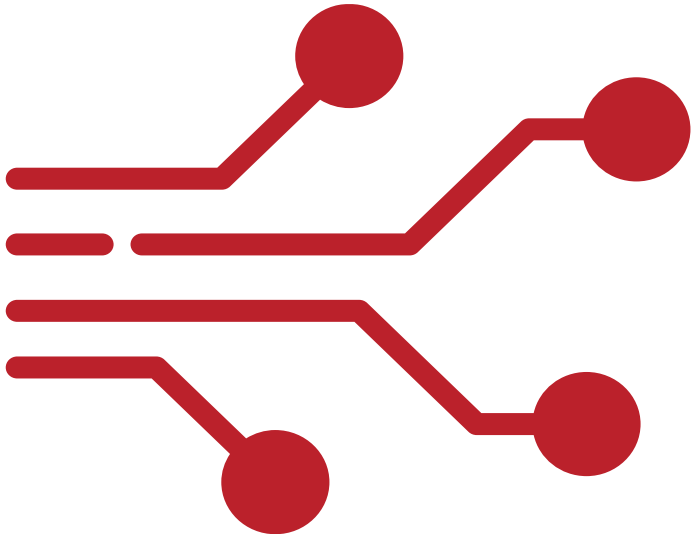
wiadomość miała sens tylko po nawinięciu na wałek o odpowiedniej grubości

Odwrócone podejście z Mezopotamii

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

30

Szyfr Cezara



Juliusz Cezar używał systemu polegającego na przesunięciu liter alfabetu o stałą liczbę miejsc

3 albo -1

szyfr podstawieniowy

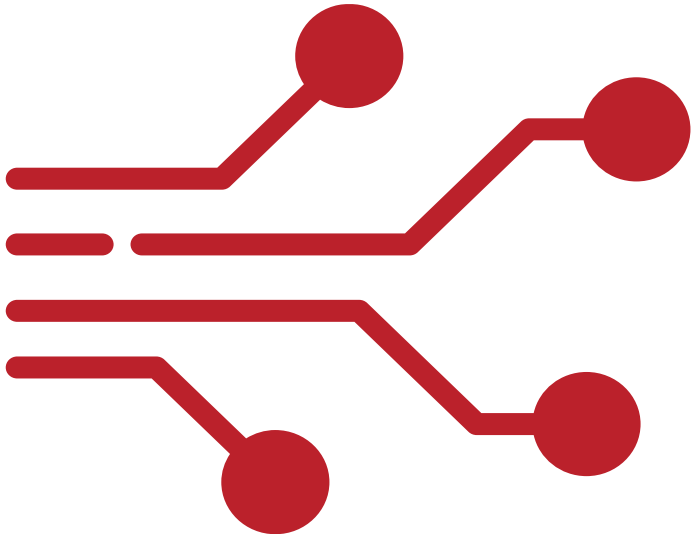
dziś wydaje się banalny, ale w czasach, gdy większość populacji była niepiśmienna, zapewniał wystarczające bezpieczeństwo komunikacji

wojska rosyjskie używały szyfru Cezara (lub jego bardzo bliskich wariantów) jeszcze w 1915 roku

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

31

Szyfr Vigenère'a



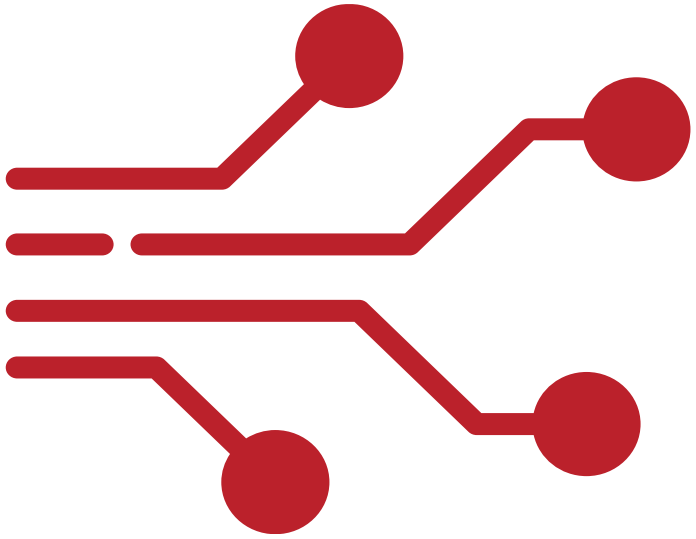
Blaise de Vigenère spopularyzował szyfr polialfabetyczny, który używał słowa-klucza do zmiany alfabetu podstawieniowego dla każdej kolejnej litery

Przez blisko 300 lat uważano go za niemożliwy do złamania *le chiffre indéchiffrable*

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

32

Era Cyfrowa Standard DES



pierwszy powszechny algorytm symetryczny, który był publicznie znany, co stanowiło praktyczną realizację zasady Kerckhoffsa

1972 start programu zabezpieczania informacji Narodowe Biuro Standardów USA

1973 ogłoszenie zapotrzebowania

1974 ponowne ogłoszenie zapotrzebowania

1975 DES zaprojektowany przez IBM

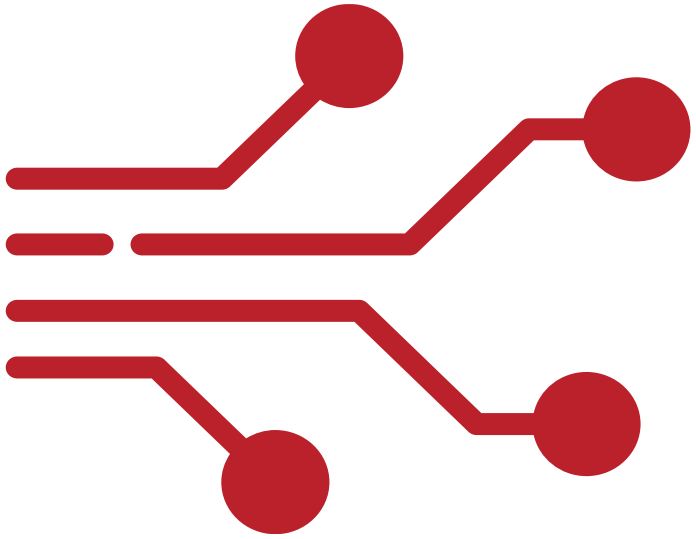
1976 roku rząd USA przyjął DES (Data Encryption Standard)

2001 opracowanie AES

2005 wycofanie DES jako standardu federalnego

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Rewolucja klucza publicznego



1976 Whitfield Diffie i Martin Hellman wymiana kluczy

1977 Algorytm Rivest-Shamir-Adleman (RSA) kryptosystem asymetryczny

Ciekawostka:

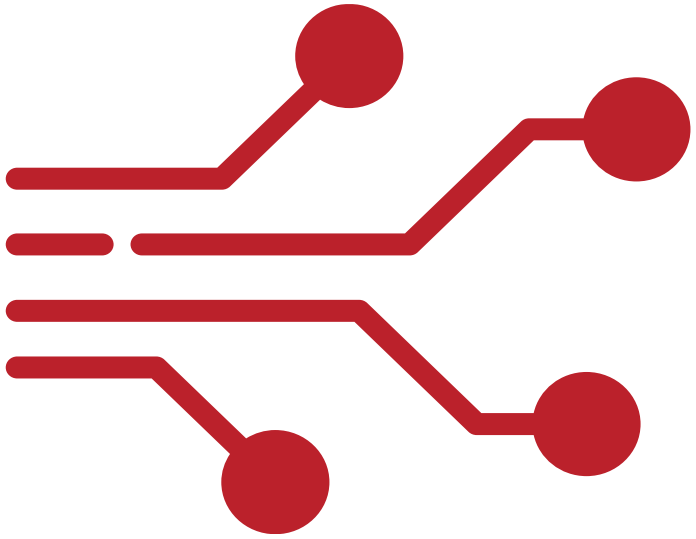
1973 Clifford Cocks z wywiadu brytyjskiego opisał podobny system, ale nie został on wdrożony. Informację o tym odtajniono dopiero w 1997

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

34

Czasy współczesne i przyszłość



Obecnie standardem jest **AES** (następca DES), a bezpieczeństwo opiera się na kryptografii krzywych eliptycznych (**ECC**).

Największym wyzwaniem staje się teraz **kryptografia postkwantowa**, która ma chronić nasze dane przed potencjalnym złamaniem przez komputery kwantowe w przyszłości

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

35

Dziękuję za uwagę

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Podstawy kryptografii
Wykład nr 2
Temat: Szyfrowanie symetryczne

dr Michał Dolecki
Katedra Inteligencji Obliczeniowej
Zakład Uczenia Maszynowego

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

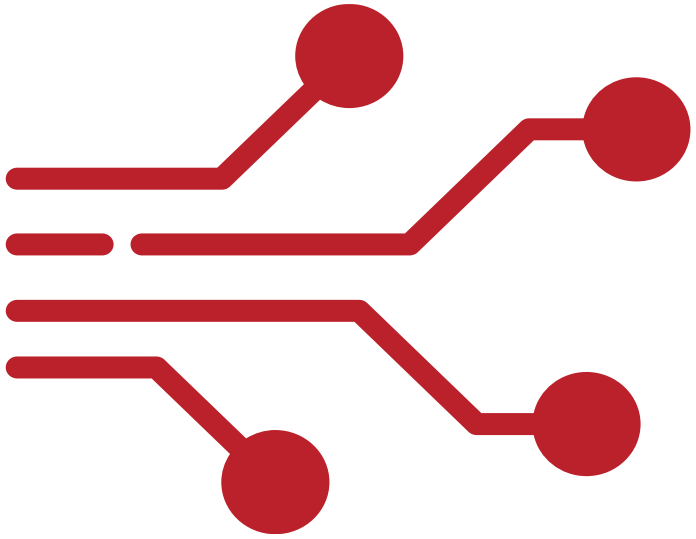
Plan wykładu

- Paradoks kryptografii symetrycznej
- Grupa cykliczna
- Algorytm iteracyjnego podnoszenia do kwadratu
- Protokół Diffiego – Hellmana
- Algorytm AES

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Kryptografia symetryczna



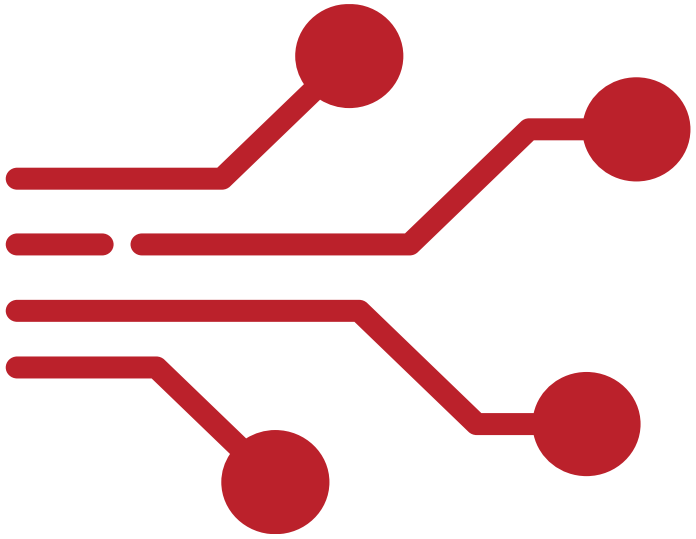
- Kryptografia symetryczna to najstarsza i najbardziej intuicyjna gałąź kryptografii
- jej istota sprowadza się do tego, że ta sama tajemnica (klucz) służy zarówno do zaszyfrowania wiadomości, jak i do jej odszyfrowania
- klucz szyfrujący i deszyfrujący są identyczne (lub można łatwo z nich wzajemnie wyliczyć np. szyfr Cezara +3 i -3)
- przypomina to skrzynię i jeden klucz, który ją zamyka i otwiera

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

3

Kryptografia symetryczna



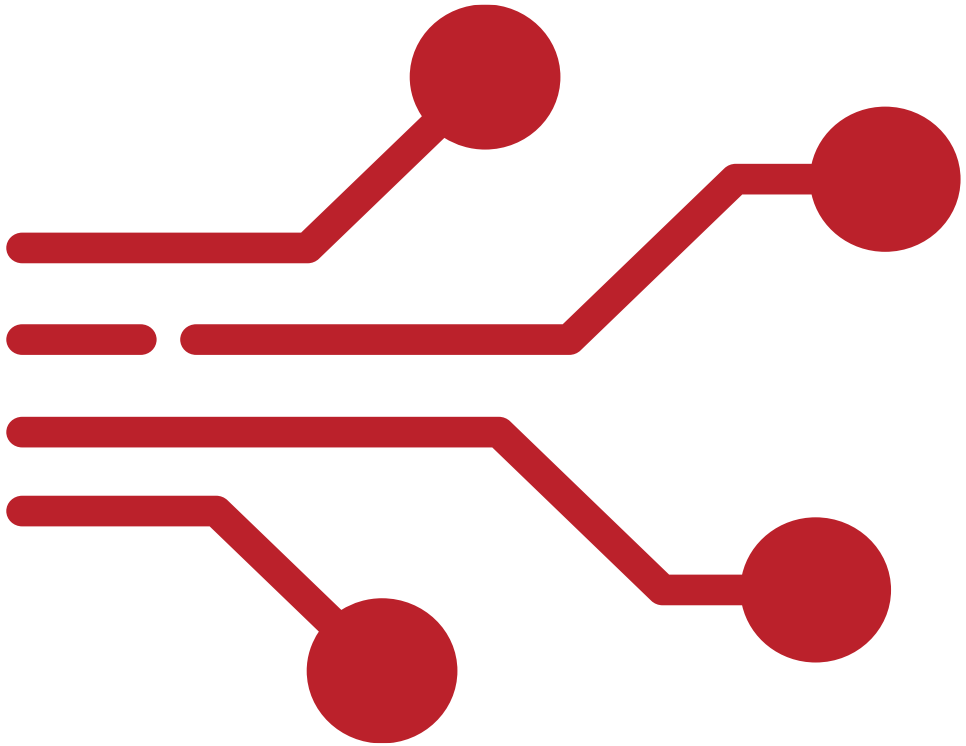
- realizuje zasadę sformułowana przez Auguste'a Kerckhoffsa w XIX wieku: system kryptograficzny powinien pozostać bezpieczny, nawet jeśli przeciwnik zna wszystkie szczegóły jego działania z wyjątkiem samego klucza
- bezpieczeństwo nie może polegać na tajności algorytmu, ale wyłącznie na tajności klucza
- pozwala projektować, analizować i publicznie dyskutować o algorytmach takich jak AES, bez obawy, że ich publiczne ujawnienie ja je osłabi

4

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

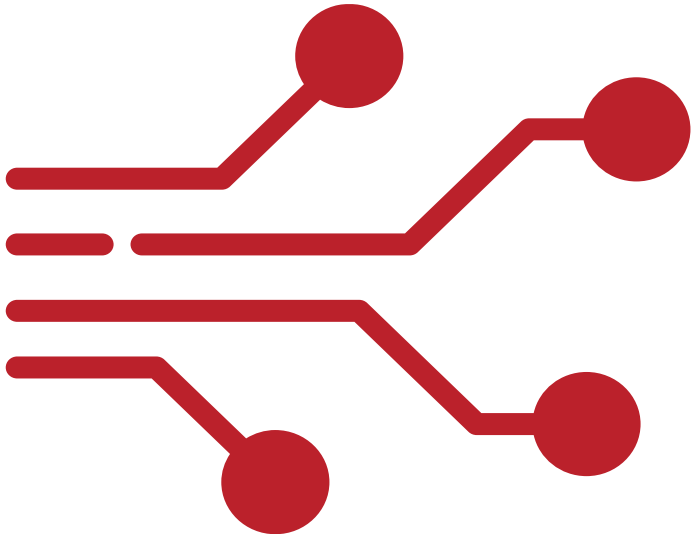
Paradoks kryptografii symetrycznej



Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

5

Paradoks kryptografii symetrycznej



- Aby móc bezpiecznie komunikować się kanałem publicznym (np. internet), musimy zaszyfrować dane
- Aby zaszyfrować dane, nadawca i odbiorca muszą posiadać ten sam, tajny klucz symetryczny
- Aby ustalić ten wspólny tajny klucz, musimy go sobie przekazać
- Przekazanie klucza kanałem publicznym jest niebezpieczne

Wniosek

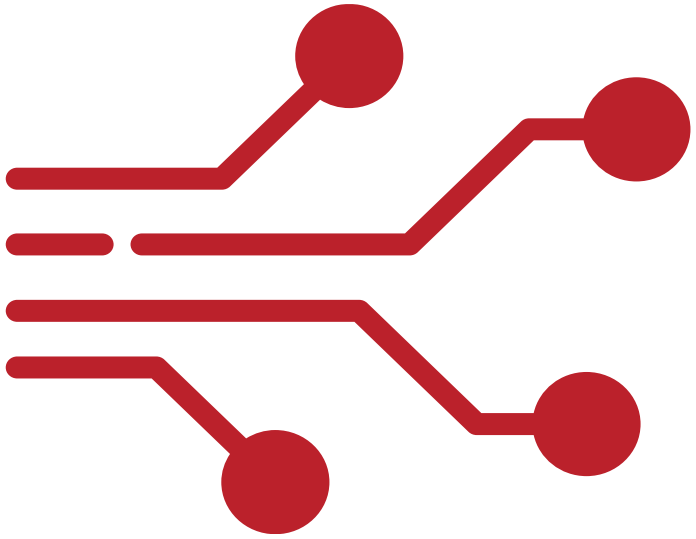
- Musimy mieć bezpieczny kanał do przekazania klucza

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

6

Paradoks kryptografii symetrycznej



- Chcemy zbudować bezpieczny kanał komunikacji
- Do jego zbudowania potrzebujemy bezpiecznego kanału do dystrybucji klucza

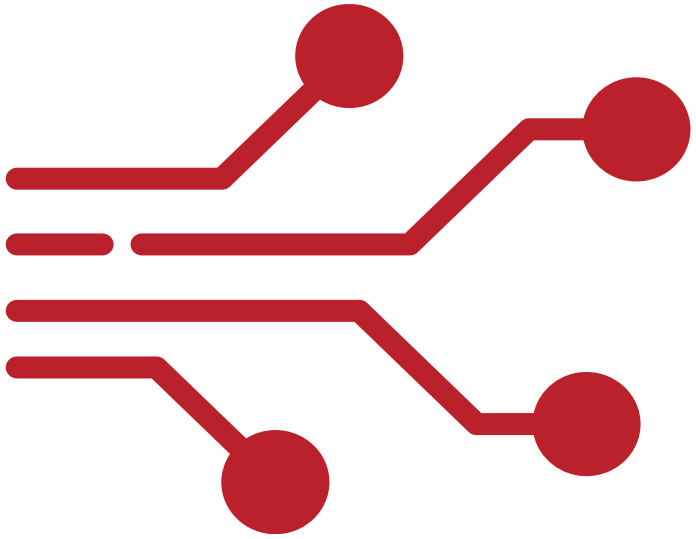
- Potrzebujemy bezpiecznego kanału, żeby móc zacząć używać bezpiecznego kanału

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

7

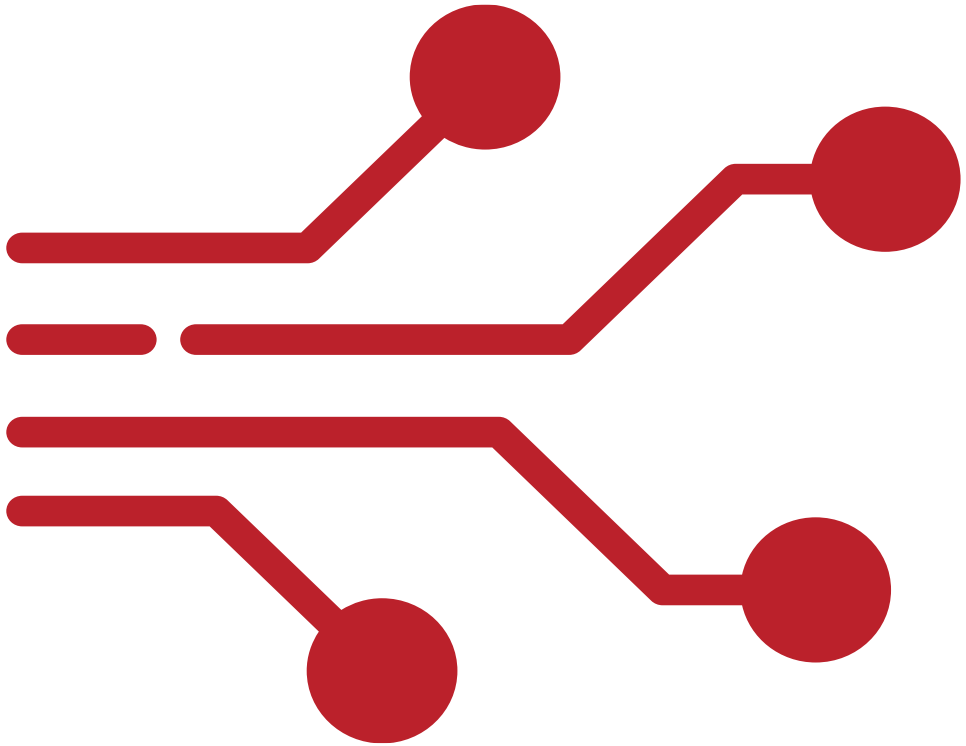
Rozwiązanie



- Historycznie do lat 70. XX wieku jedynym praktycznym rozwiązaniem było fizyczne przekazanie klucza (kurier, spotkanie). Metoda kosztowna, powolna i nie skalowalna
- Protokół Diffiego-Hellmana (Diffie-Hellmana) umożliwia uzgodnienie wspólnego sekretu (klucza), komunikując się wyłącznie przez jawny, publiczny kanał, bez wcześniejszego uzgodnienia tajemnicy

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Grupa cykliczna

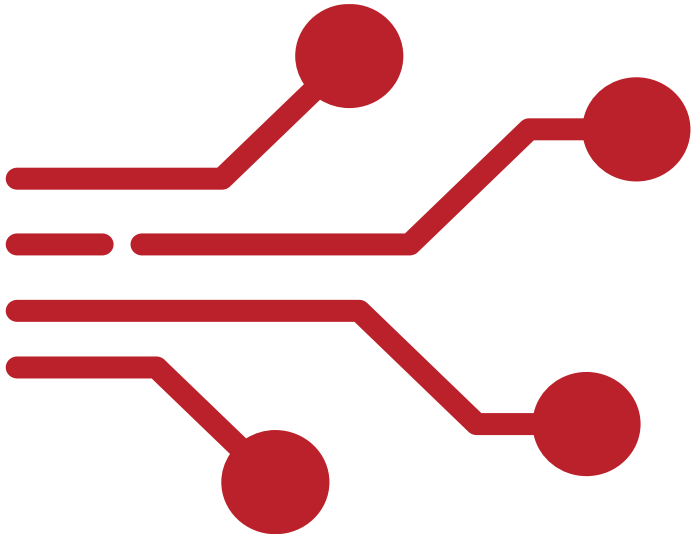


Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

9

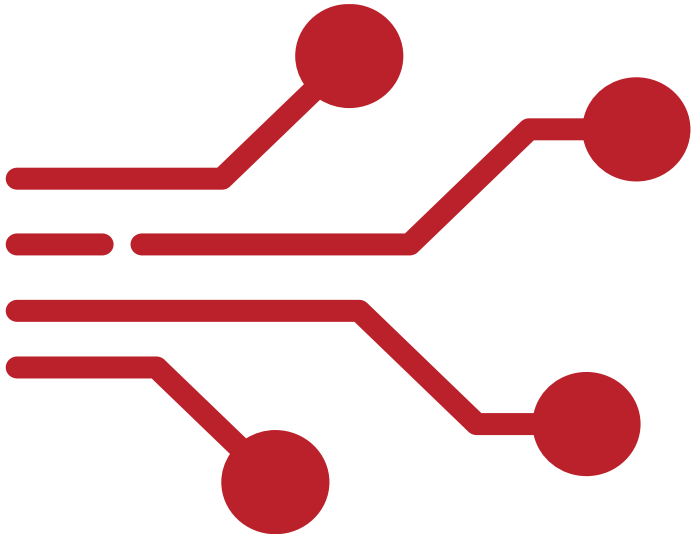
Grupa cykliczna z generatorem



- Spójrzmy na kolumnę dla generatora g = 2
- Wartości w tej kolumnie to: [2, 4, 8, 5, 10, 9, 7, 3, 6, 1]
- Jest to ciąg wyników potęgowania liczby 2 modulo 11 dla kolejnych wykładników
- Działanie w przód jest proste i szybkie: jeśli chcę wiedzieć, ile wynosi 2^6 mod 11, wykonuję obliczenia (6 kroków) i otrzymuję wynik 9
- Załóżmy, że ktoś podaje mi liczbę y = 9 i pyta: „Jaki musi być wykładnik x, aby przy podstawie 2 otrzymać 9?”
- Jest to łatwe, bo tabelka jest mała i mamy ją przed oczami 10

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Problem matematyczny



- A teraz bez tabelki :)
- „Jaki musi być wykładnik x, aby przy podstawie 2 otrzymać 3 potęgując mod 11?”
- Matematycznie $\log_2 3 \, mod 11$
- Sedno problemu logarytmu dyskretnego polega na tym, że dla odpowiednio dużych liczb (rzędu setek czy tysięcy bitów) to odwrotne działanie jest praktycznie niewykonalne w rozsądnym czasie

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

11

Problem logarytmu dyskretnego

(*Discrete Logarithm Problem, DLP*)

Problem trudny obliczeniowo, na którym opiera się bezpieczeństwo protokołu Diffiego-Hellmana i wielu innych systemów kryptografii asymetrycznej

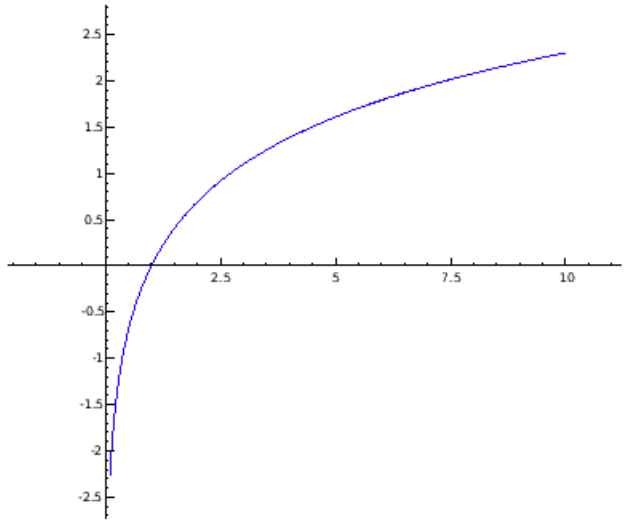
- Obliczenie potęgi (g^x mod p) jest łatwe i szybkie.
- Odtworzenie wykładnika (x) na podstawie znanych g, p i wyniku (y) jest obliczeniowo trudne.

12

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Funkcja logarytmiczna



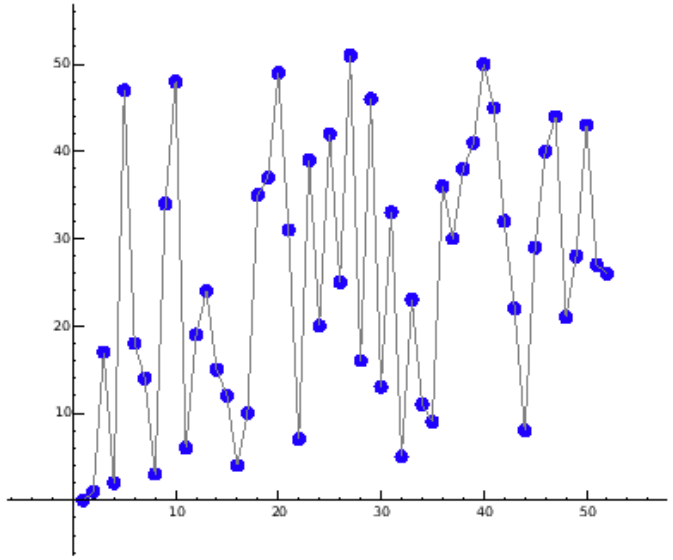


Figure 3.2: Graphs of the continuous log and of the discrete log modulo 53 .Which looks easier to compute?

Źródło: https://wstein.org/edu/2007/spring/ent/ent-html/node35.html

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Realne wartości liczb 2048b

2048-bit MODP Group

This group is assigned id 14.

This prime is: 2^2048 - 2^1984 - 1 + 2^64 * { [2^1918 pi] + 124476 }

Its hexadecimal value is:

FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D
C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F
83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D
670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B
E39E772C 180E8603 9B2783A2 EC07A28F B5C55DF0 6F4C52C9
DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510
15728E5A 8AACAA68 FFFFFFFF FFFFFFFF

14

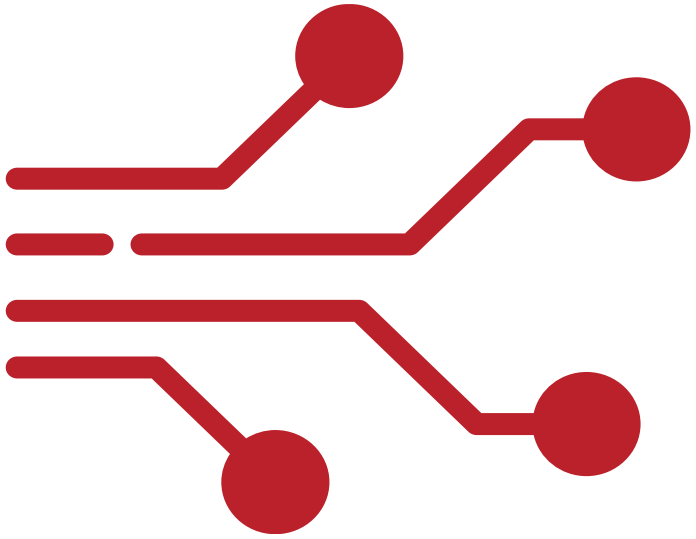
The generator is: 2.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Realne wartości liczb w kryptografii

W systemie dziesiętnym

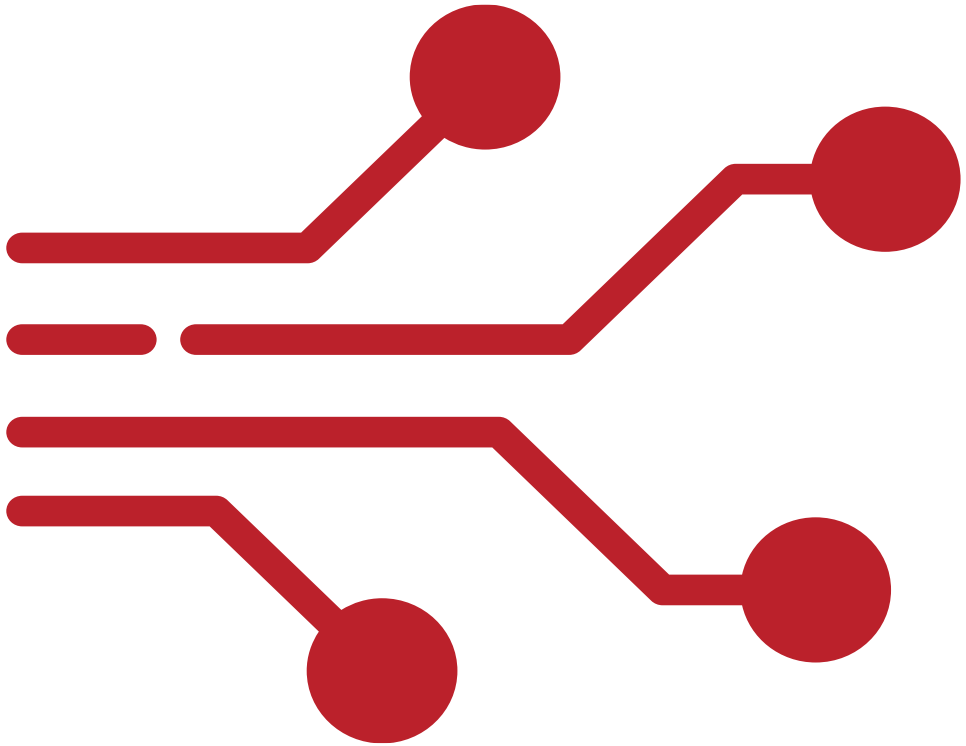


232989263058430097782333066929949666991953250529884813583279123049182377594957605988118025287739572879357672159670068370165985836001097240310461876800008320491295988981666872506869186638090714775871261356780720493721345095810667355157155026938258296238645511394528157745781206103632115160167389178201216694827051412030113697960308331189993356050519106093539912056976662705626958434771032338668478143242702758178129045763955639352125585093121543781504930604163931165389656157177726330089849311397850020164228943538743110547671049281514495811776823321946029288174780517726593920677599026367332219436701546731998593457 5

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Algorytm iteracyjnego podnoszenia do kwadratu



Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

16

Algorytm szybkiego potęgowania

Algorytm iteracyjnego podnoszenia do kwadratu (ang. *iterative squaring*), znany również jako algorytm szybkiego potęgowania modularnego (ang. *modular exponentiation*), służy do efektywnego obliczania wyrażenia:

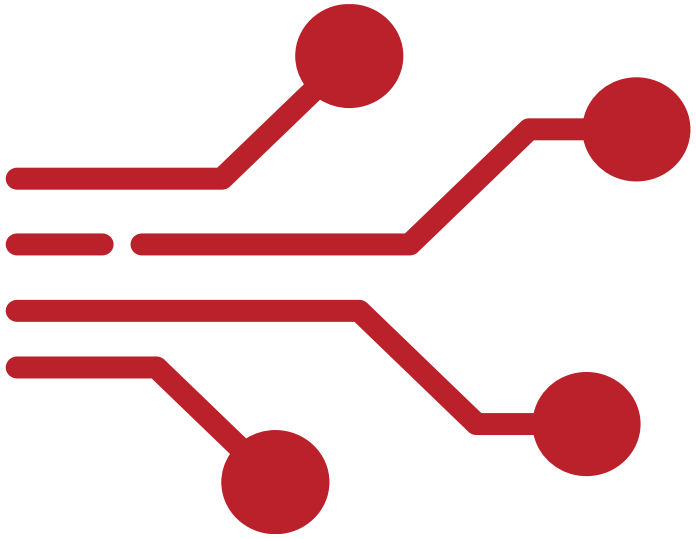
$$a^b \ mod \ n$$

gdzie a jest podstawą, b wykładnikiem (często bardzo dużą liczbą), a n modułem.

Dzięki wykorzystaniu praw potęgowania oraz operacji modulo, a także systemu binarnego, algorytm ten ma złożoność obliczeniową $O(log_2 b)$ i jest jednym z piękniejszych algorytmów w informatyce.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Podstawy matematyczne - potęgi



- Prawo potęgowania dla iloczynu

$$a^{x+y} = a^x \cdot a^y.$$

- Prawo potęgowania dla potęgi potęgi

$$(a^x)^y = a^{x \cdot y}.$$

Szczególnie istotne jest

$$\left(a^{2^k}\right)^2 = a^{2^{k+1}},$$

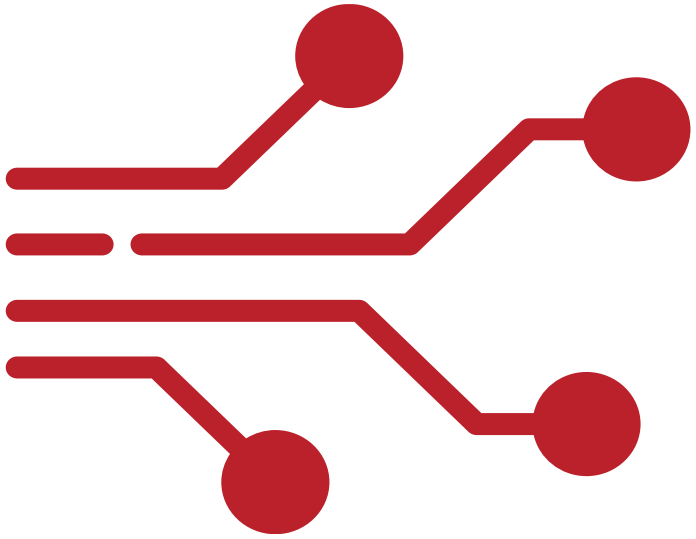
co pozwala nam uzyskiwać kolejne potęgi przez ciągłe podnoszenie do kwadratu.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

18

Podstawy matematyczne – modulo



- Własności modulo dla mnożenia

$$(a \cdot b)\ mod\ n = [(a\ mod\ n) \cdot (b\ mod\ n)]\ mod\ n$$

oraz

$$a^k\ mod\ n = (a\ mod\ n)^k\ mod\ n$$

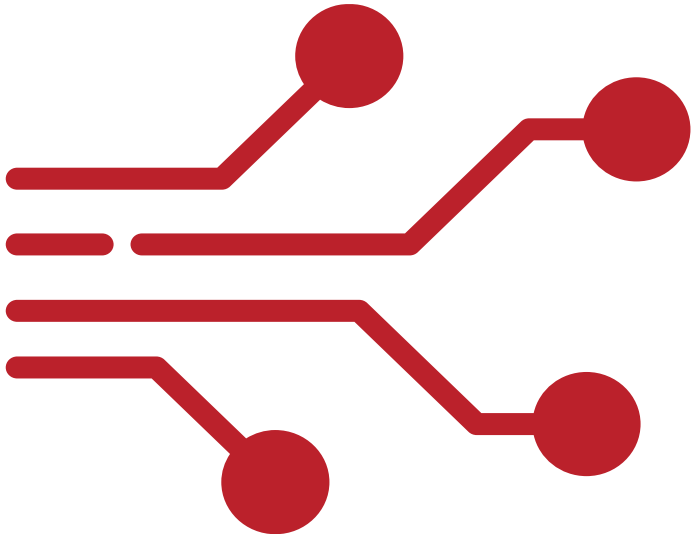
Dzięki tym własnościom możemy wykonywać wszystkie obliczenia w ciele reszt modulo n, unikając ogromnych liczb pośrednich.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

19

Idea algorytmu



Kluczowym pomysłem jest przedstawienie wykładnika b w systemie binarnym:

$$b = b_{k-1}b_{k-2} \dots b_1 b_0 \text{ (gdzie } b_i \in \{0, 1\})$$

Wtedy

$$a^b = a^{\sum_{i=0}^{k-1} b_i \cdot 2^i} = \prod_{i=0}^{k-1} a^{b_i \cdot 2^i}$$

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

20

Wyjaśnienie oznaczeń

Jak rozumieć to cudo $\prod_{i=0}^{k-1} a^{b_i \cdot 2^i}$ - przykład

- Niech:
- $a = 5$
- $b = 11$
- k = liczba bitów b

Uwaga!!!

To jeszcze nie jest pełny algorytm – brakuje modulo!!!

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

21

Krok 1: Zamiana b na system binarny

$$11_{10} = 1011_2$$

To oznacza:

$b_3 = 1$ dla $2^3 = 8$

$b_2 = 0$ dla $2^2 = 4$

$b_1 = 1$ dla $2^1 = 2$

$b_0 = 1$ dla $2^0 = 1$

Zatem:

$$b = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 8 + 0 + 2 + 1 = 11$$

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Krok 2: Zastosowanie wzoru

Zgodnie ze wzorem:

$$5^{11} = 5^{(1\cdot 2^3+0\cdot 2^2+1\cdot 2^1+1\cdot 2^0)} = 5^{1\cdot 2^3} \cdot 5^{0\cdot 2^2} \cdot 5^{1\cdot 2^1} \cdot 5^{1\cdot 2^0}$$

Prawa strona to $\prod_{i=0}^{k-1} a^{b_i \cdot 2^i}$

Czyli:

$$5^{11} = 5^8 \cdot 5^0 \cdot 5^2 \cdot 5^1$$

Ponieważ $5^0 = 1$ bo $b_2 = 0$,(możemy pominąć ten czynnik (mnożenie przez 1 nic nie zmienia):

$$5^{11} = 5^8 \cdot 5^2 \cdot 5^1$$

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

23

Krok 3: Obliczenie każdego czynnika (doliczenie wyniku)

$$5^1 = 5$$
$$5^2 = 25$$
$$5^4 = (5^2)^2 = 25^2 = 625$$
$$5^8 = (5^4)^2 = 625^2 = 390625$$

Krok 4: Mnożenie

$$5^{11} = 5^8 \cdot 5^2 \cdot 5^1 = 390625 \cdot 25 \cdot 5$$

Wynik

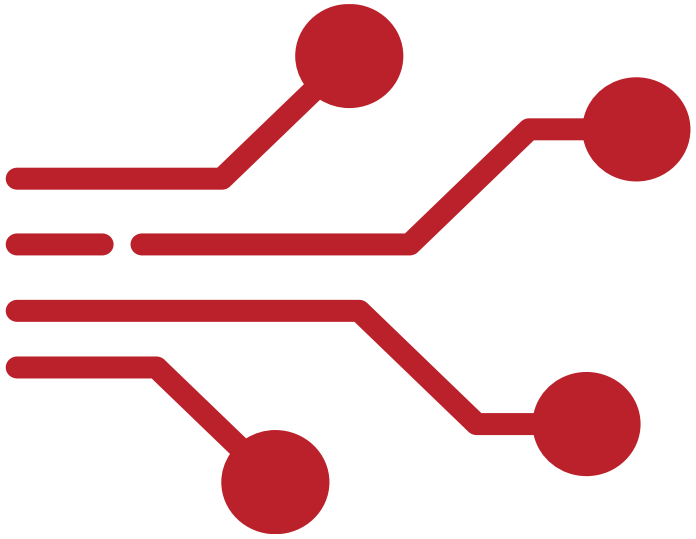
$$5^{11} = 48828125$$

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

24

Pełna wersja algorytmu



Wracając do opisu algorytmu

Ponieważ b_i jest równe 0 lub 1, to $a^{b_i \cdot 2^i}$ jest równe:

- 1, jeśli $b_i = 0$
- a^{2^i}, jeśli $b_i = 1$

  Dotyczy to również początkowego a dla b_0

Zatem:

$$a^b mod\ n = \left(\prod_{i:\ b_i=1} a^{2^i} \right) mod\ n$$

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

25

Potęgowanie iteracyjne

Wartości a^{2^i} możemy obliczać iteracyjnie:

- $a^{2^0} = a^1 = a$
- $a^{2^1} = \left(a^{2^0}\right)^2$
- $a^{2^2} = \left(a^{2^1}\right)^2$
- ogólnie $a^{2^{i+1}} = \left(a^{2^i}\right)^2$

Każdy krok to podniesienie do kwadratu poprzedniego wyniku, a w każdym kroku możemy użyć operacji modulo aby wynik pozostał w ustalonym przedziale

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Przykład obliczeniowy

Dodając do przykładu np. mod31 mamy

(a^k) mod n =	25

a	5
k	11
n	31

	a'	b	k_2
0	5	5	1
1	25	1	1
2	5	1	0
3	25	25	1

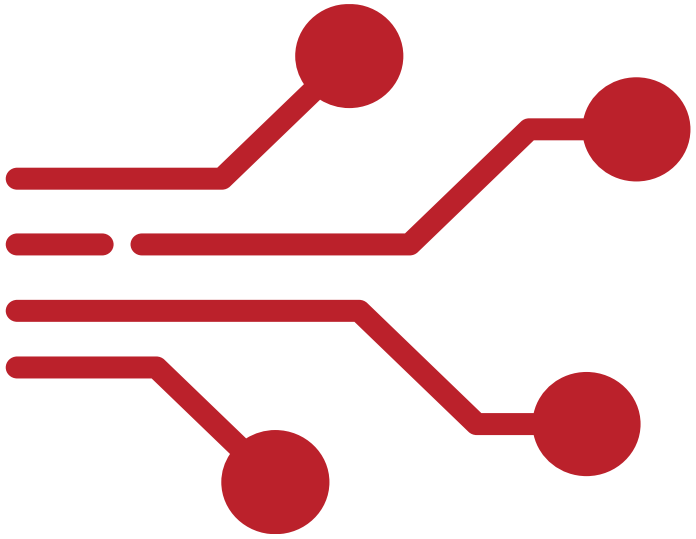
Źródło: opracowanie własne

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

27

Złożoność i zalety algorytmu



- **Liczba iteracji**: równa liczbie bitów b, czyli $O(log_2 b)$.
- **Operacje**: w każdej iteracji co najwyżej dwa mnożenia modularne (jedno dla wyniku, jedno dla podstawy).
- **Korzyść**: unikamy przechowywania ogromnych liczb dzięki modulo po każdej operacji.

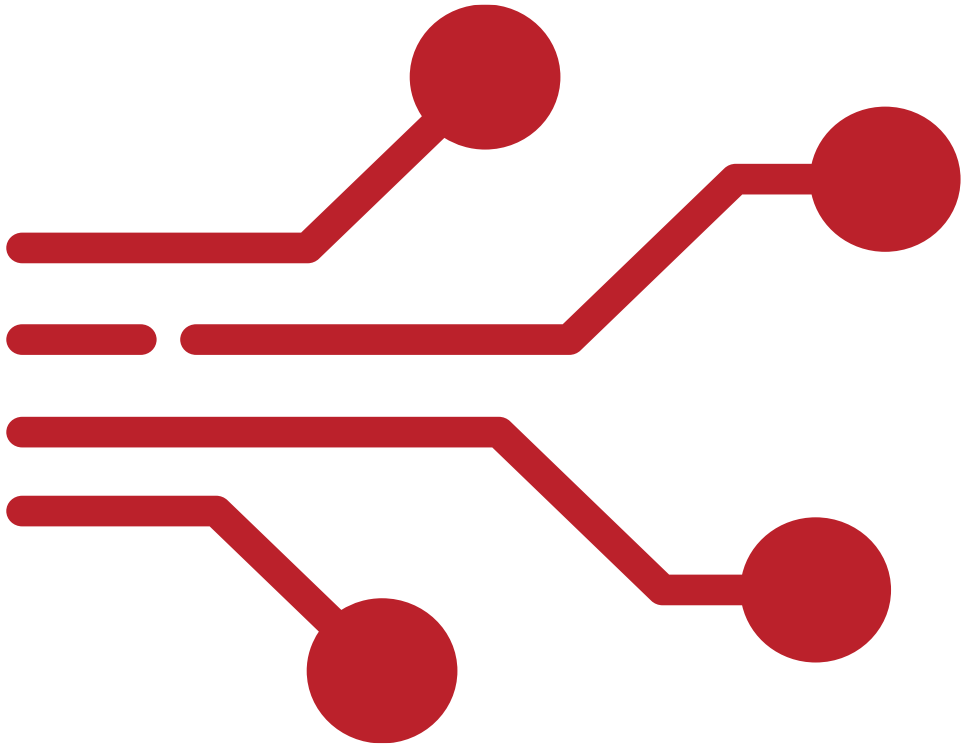
Algorytm ten jest powszechnie stosowany w kryptografii (np. RSA, Diffie-Hellman) do szybkiego obliczania potęg w ciałach skończonych.

28

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

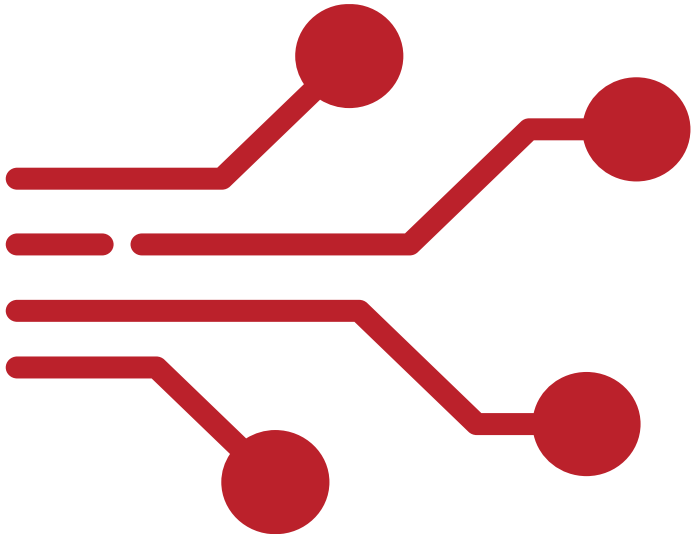
Protokół Diffiego – Hellmana



Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

29

Wiadomości podstawowe



- Bailey Whitfield "Whit" Diffie
- Martin Hellman
- 1976 protokół uzgadniania kluczy szyfrujących w otwartym kanale komunikacyjnym
- Opiera się na problemie logarytmu dyskretnego

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Algorytm Diffiego – Hellmana

- Alicja i Bob uzgadniają ze sobą dwie liczby: liczbę p, która jest możliwie dużą liczbą pierwszą oraz liczbę g, która jest generatorem grupy Z_p:
- Alicja wybiera dużą liczbę całkowitą a taką, że a<p-1 i wysyła do Boba

$$x = g^a (mod\ p);$$

- Bob wybiera losowo dużą liczbę całkowitą b taką, że b<p-1 i wysyła do Alicji

$$y = g^b (mod\ p);$$

- Alicja po otrzymaniu od Boba y oblicza swój klucz:

$$K = y^a (mod\ p);$$

- Bob w ten sam sposób oblicza swój klucz, który jest identyczny z kluczem Alicji:

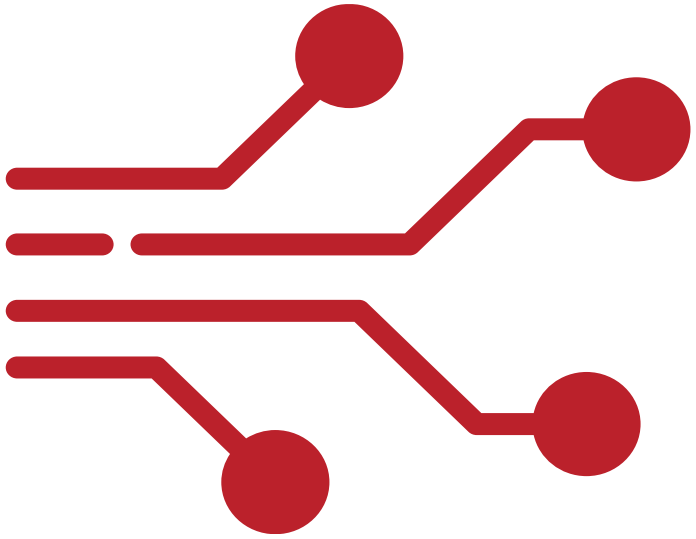
$$K = x^b (mod\ p);$$

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

31

Uzasadnienie



Uzasadnienie działania protokołu Diffiego – Hellmana opiera się na podstawowych zasadach matematycznych

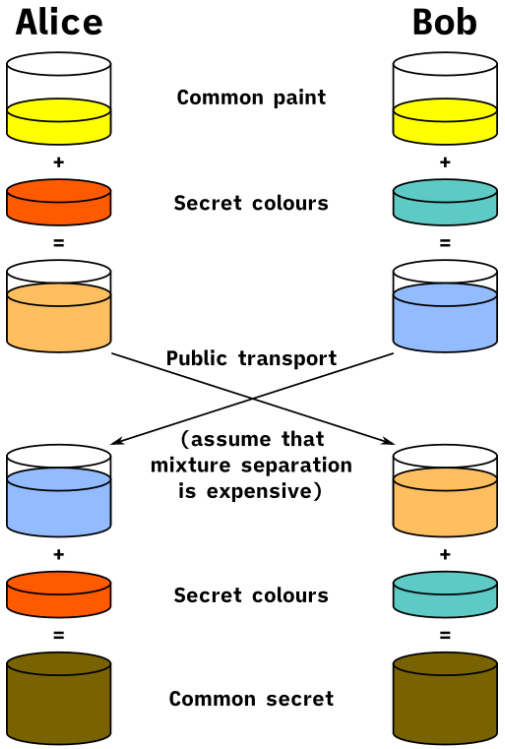
- $K = y^a (mod\ p) = \left(g^b\right)^a (mod\ p) = g^{ba} (mod\ p)$
- $K = x^b (mod\ p) = (g^a)^b (mod\ p) = g^{ab} (mod\ p)$

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

32

Ilustracja działania algorytmu



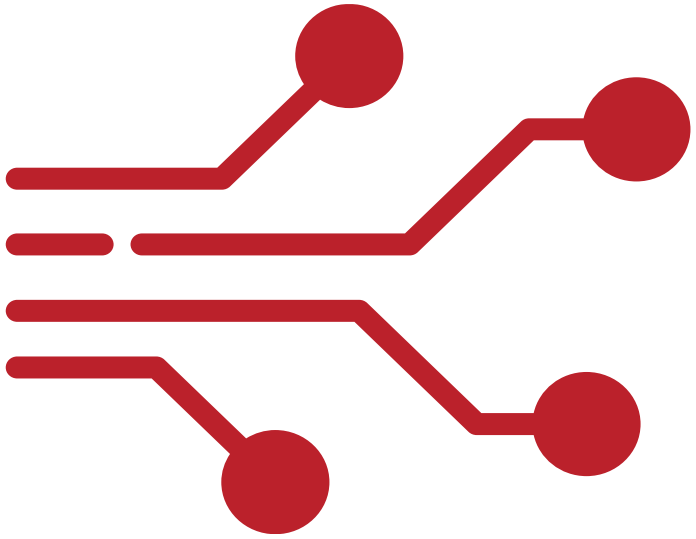
Źródło: https://pl.wikipedia.org/wiki/Protok%C3%B3%C5%82_Diffiego-Hellmana

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

33

Przykład obliczeniowy



- Alicja i Bob uzgadniają ze sobą dwie liczby: liczbę p =23, która jest możliwie dużą liczbą pierwszą oraz liczbę g=5, która jest generatorem grupy Z_p:
- Alicja wybiera dużą liczbę całkowitą a=6 i wysyła do Boba

$$x = 5^6 (mod\ 23) = 8$$

- Bob wybiera losowo dużą liczbę całkowitą b=19 i wysyła do Alicji

$$y = 5^{19} (mod\ 23) = 7$$

- Alicja po otrzymaniu od Boba y oblicza swój klucz:

$$K = 7^6 (mod\ 23) = 4$$

- Bob w ten sam sposób oblicza swój klucz, który jest identyczny z kluczem Alicji

$$K = 8^{19} (mod\ 23) = 4$$

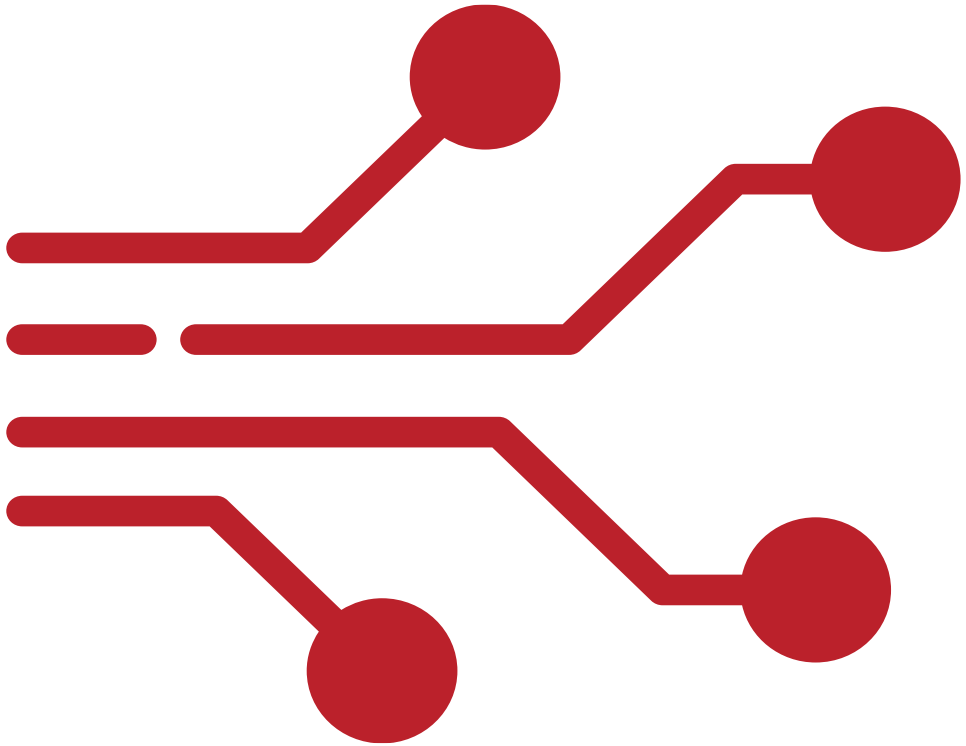
Alicja i Bob Ustalili swój własny klucz szyfrujący.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

34

Algorytm AES

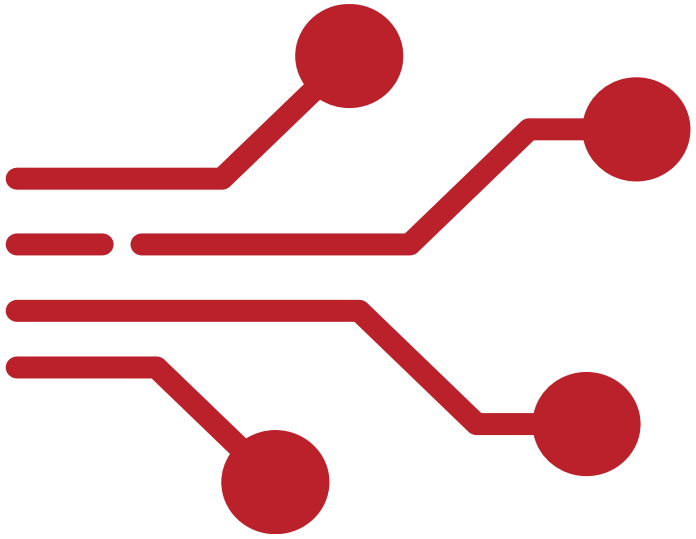


Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

35

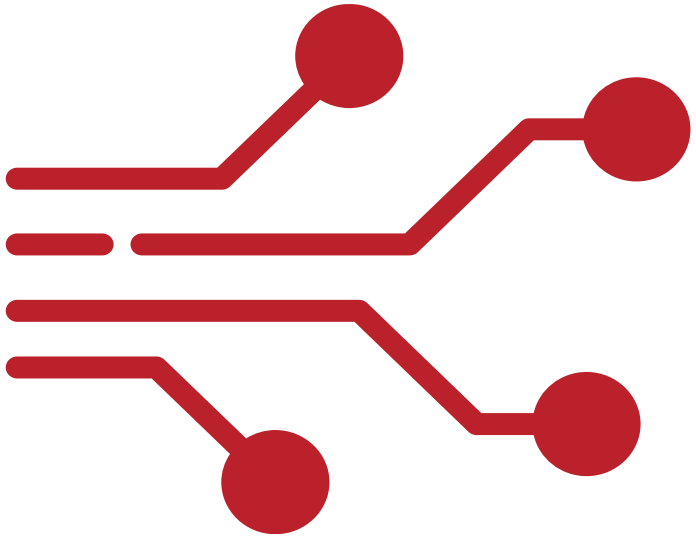
Wiadomości podstawowe



- AES(Advanced Encryption Standard, oryginalnie Rijndael) jest to symetryczny szyfr blokowy zaprojektowany przez belgijskich kryptologów Vincenta Rijmena i Joana Daemena
- Szyfr blokowy – szyfruje dane w blokach o stałej długości
- Blok danych: 128 bitów (16 bajtów)
- Długość klucza: 128, 192 lub 256 bitów
- Liczba rund zależy od długości klucza: 10 (dla 128), 12 (dla 192), 14 (dla 256)
- Następca DES
- AES używamy do ochrony transakcji internetowych, transmisji bezprzewodowych i danych przechowywanych lokalnie

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Historia powstania



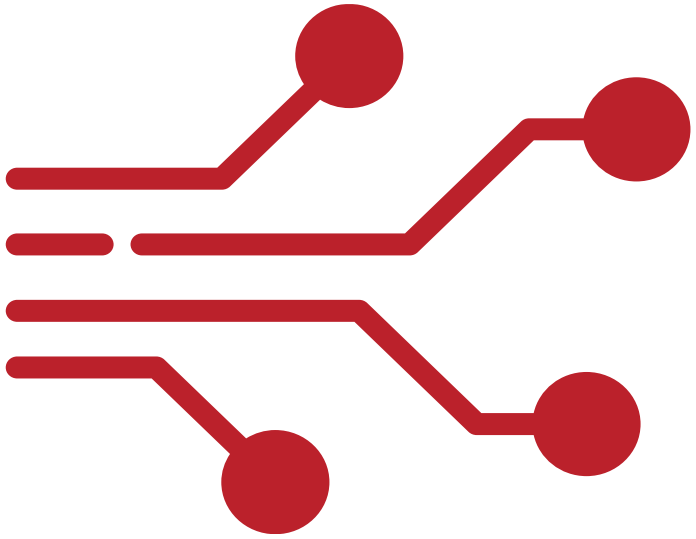
- 1997 NIST (ang. National Institute of Standards and Technology) ogłosił konkurs na nowy standard federalny USA, ponieważ dotychczasowy standard federalny jeśli chodzi o szyfry – DES przestał być wystarczająco bezpieczny do szyfrowania informacji o najwyższym poziomie poufności
- DES, a dokładniej Lucifer po ponad dwudziestu latach użytkowania, ze względu na nieustannie rosnącą moc obliczeniową komputerów oraz coraz skuteczniejsze metody kryptoanalizy nie oferował już wystarczającego bezpieczeństwa

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

37

Historia powstania



- Do konkursu zgłoszono piętnaście algorytmów szyfrujących.
- Do finalnej potyczki stanęły:
  - Rijndael,
  - RC6,
  - Mars,
  - Serpent
  - Twofish.
- Po pięciu latach dokładnego oceniania zgłoszonych projektów ogłoszono zwycięstwo algorytmu Rijndael
- W 2002 roku stał się oficjalnie standardem federalnym i jednocześnie zyskał nową nazwę AES.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Reprezentacja danych

Zorganizowanie danych w odpowiedniej strukturze. Blok 128 bitów (16 bajtów) układa się w macierz 4×4 bajtów, zwaną stanem (state):

Wejściowe bajty: [b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15]

Macierz stanu (wypełniana kolumnami):

b0	b4	b8	b12
b1	b5	b9	b13
b2	b6	b10	b14
b3	b7	b11	b15

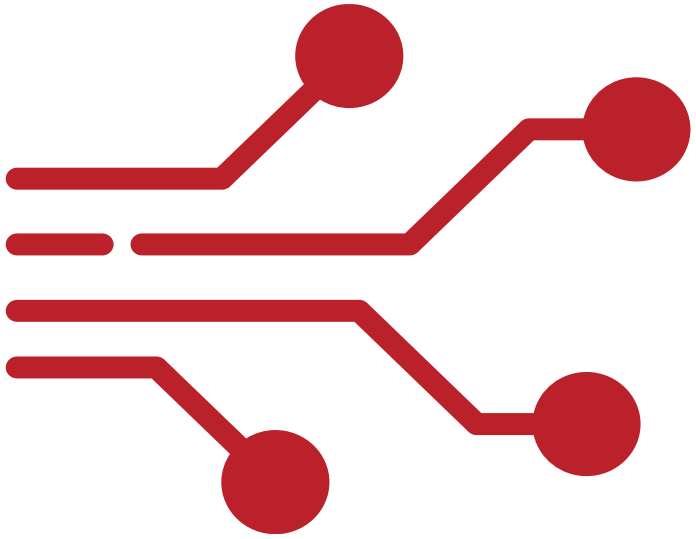
← kolumna 0, potem 1, itd.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

39

Struktura szyfrowania



Szyfrowanie AES to sekwencja powtarzalnych rund. Każda runda (oprócz ostatniej) składa się z czterech operacji:

1. SubBytes – podstawianie bajtów (zamiana każdego bajtu na inny według tabeli)
2. ShiftRows – przesuwanie wierszy
3. MixColumns – mieszanie kolumn (pominięte w ostatniej rundzie)
4. AddRoundKey – dodanie klucza rundy

Przed pierwszą rundą wykonujemy dodatkowe AddRoundKey (inicjalizacja).

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Krok 0: Rozszerzanie klucza (Key Expansion)

Zanim zaczniemy właściwe szyfrowanie, z głównego klucza (np. 128-bitowego) generujemy osobne klucze dla każdej rundy. Dla 10 rund potrzebujemy 11 kluczy (jeden inicjalny + 10 rundowych). Każdy klucz rundy ma dokładnie 128 bitów (16 bajtów).

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

41

Krok 1: SubBytes – podstawianie bajtów

Każdy z 16 bajtów w macierzy stanu jest zastępowany innym bajtem według ustalonej, niezmiennej tabeli zwanej S-Box (Substitution Box).

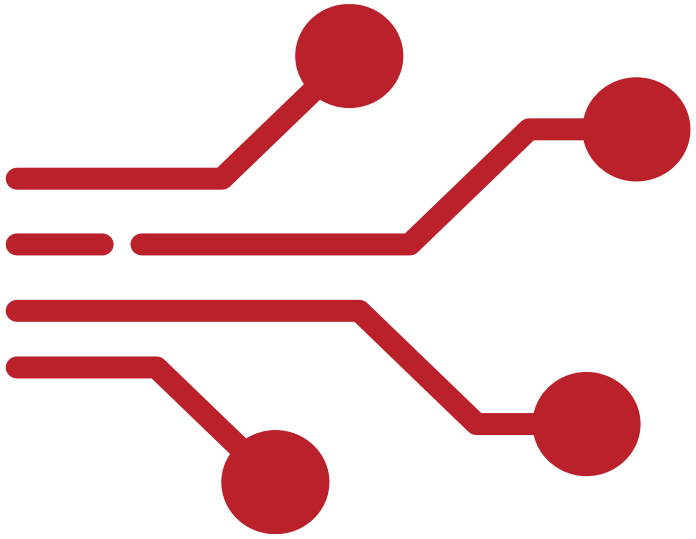
Dla przykładu: jeśli bajt ma wartość 0x53, to patrzymy do tabeli i znajdujemy nową wartość, np. 0xED.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

42

Istota SBox



Wprowadza to nieliniowość do szyfru. Gdybyśmy używali tylko operacji liniowych (jak przesunięcia i dodawania), cały szyfr dałoby się opisać prostym równaniem i *łatwo* złamać.

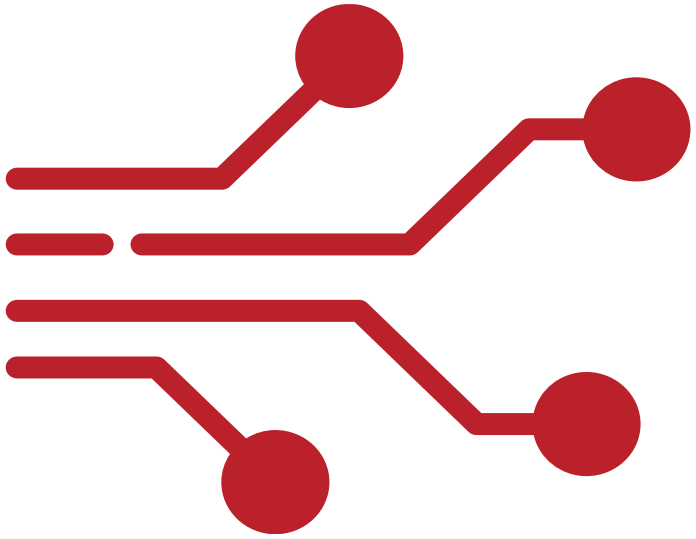
S-Box sprawia, że nawet zmiana jednego bitu na wejściu powoduje całkowicie nieprzewidywalną zmianę na wyjściu.

Ważne: Operacja jest odwracalna – przy deszyfrowaniu używamy odwrotnej tabeli (Inverse S-Box).

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

43



Krok 2: ShiftRows – przesuwanie wierszy

Wiersze macierzy stanu są przesuwane cyklicznie w lewo:

- Wiersz 0 (pierwszy) – bez przesunięcia
- Wiersz 1 – przesunięcie o 1 pozycję
- Wiersz 2 – przesunięcie o 2 pozycje
- Wiersz 3 – przesunięcie o 3 pozycje

Przed ShiftRows:

```
┌ a  b  c  d ┐
└ e  f  g  h ┘
┌ i  j  k  l ┐
└ m  n  o  p ┘
```

→

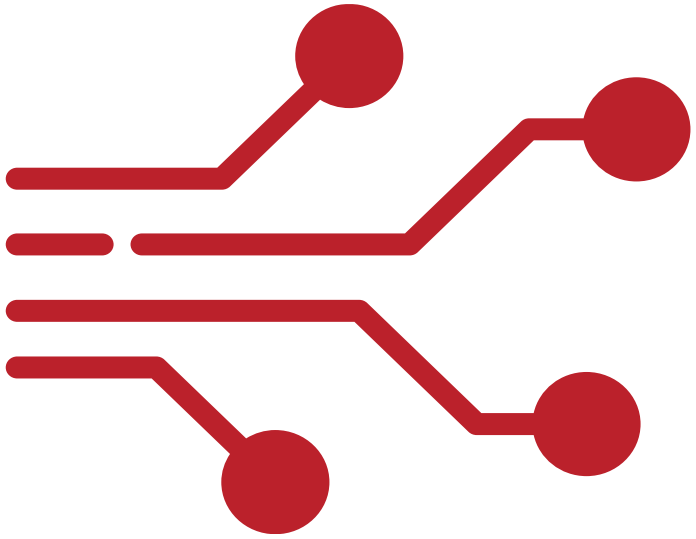
Po ShiftRows:

```
┌ a  b  c  d ┐   (bez zmian)
└ f  g  h  e ┘   (przesunięcie o 1)
┌ k  l  i  j ┐   (przesunięcie o 2)
└ p  m  n  o ┘   (przesunięcie o 3)
```


Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Znaczenie przesunięcia



To operacja, która rozrzuca bajty między kolumnami

Dzięki temu zmiana w jednym bajcie na wejściu wpływa na wiele kolumn w kolejnych rundach

Jest to tzw. dyfuzja

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

45

Krok 3

Dla każdej kolumny [a0, a1, a2, a3] obliczamy nowe wartości [b0, b1, b2, b3] według wzoru:

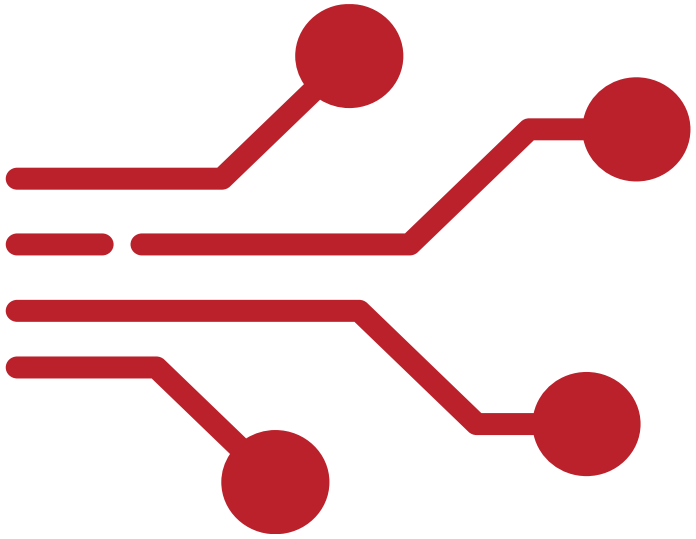
- $b0 = 2 \cdot a0 + 3 \cdot a1 + 1 \cdot a2 + 1 \cdot a3$
- $b1 = 1 \cdot a0 + 2 \cdot a1 + 3 \cdot a2 + 1 \cdot a3$
- $b2 = 1 \cdot a0 + 1 \cdot a1 + 2 \cdot a2 + 3 \cdot a3$
- $b3 = 3 \cdot a0 + 1 \cdot a1 + 1 \cdot a2 + 2 \cdot a3$

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

46

Znaczenie MixColumns



To kluczowa operacja dyfuzji – każdy bajt w kolumnie wpływa na wszystkie bajty tej kolumny po przekształceniu.

Dzięki temu po kilku rundach każdy bit wyjścia zależy od wszystkich bitów wejścia.

Uwaga: MixColumns nie występuje w ostatniej rundzie.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

47

Krok 4: AddRoundKey – dodanie klucza rundy

Bierzemy 16 bajtów aktualnego stanu i wykonujemy operację XOR z 16 bajtami klucza danej rundy (wygenerowanego wcześniej z klucza głównego).

XOR jest to operacja odwracalna (jeśli zrobimy XOR dwa razy z tym samym kluczem, wracamy do początku), szybka w implementacji sprzętowej i programowej.

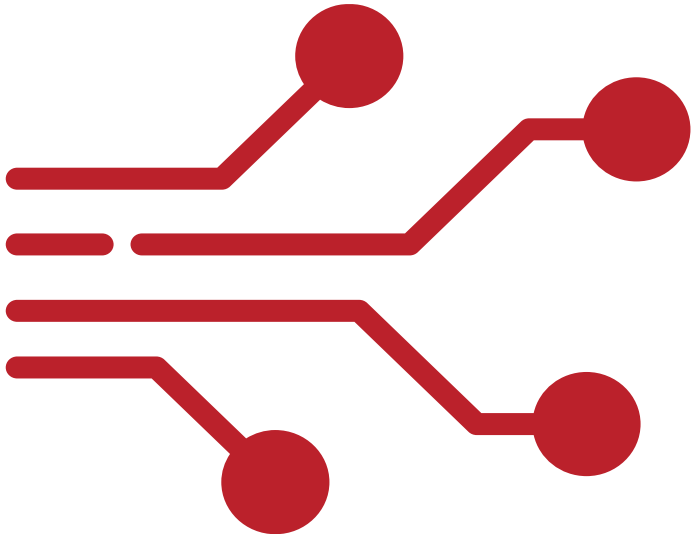
- Stan: [b0 b1 ... b15]
- Klucz: [k0 k1 ... k15]
- Wynik: [b0⊕k0, b1⊕k1, ..., b15⊕k15]

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

48

Deszyfrowanie



Deszyfrowanie wykonuje się w odwrotnej kolejności przy użyciu odwrotnych operacji:

- Inverse SubBytes (inna tabela)
- Inverse ShiftRows (przesunięcia w prawo zamiast w lewo)
- Inverse MixColumns (inna macierz mnożenia)
- AddRoundKey (to samo, bo XOR jest odwracalny)

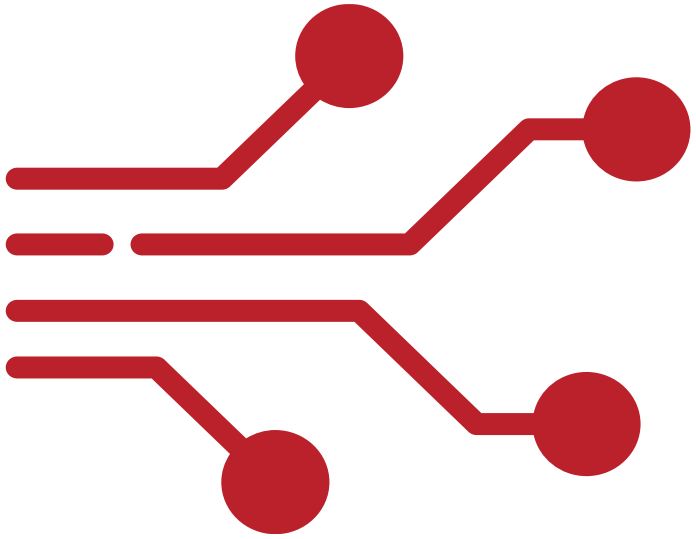
Kolejność rund jest odwrócona, a klucze używane w odwrotnej kolejności (najpierw Key10, potem Key9... aż do Key0).

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

49

Bezpieczeństwo AES



- Wszystkie operacje są odwracalne – można odzyskać dane, znając klucz
- Silna dyfuzja – po kilku rundach każdy bit wyjścia zależy od wszystkich bitów wejścia
- Nieliniowość (S-Box) – uniemożliwia opisanie szyfru prostymi równaniami
- Klucz dodawany w każdej rundzie – nawet znajomość stanu w połowie nie pozwala odtworzyć klucza
- Prostota implementacji – operacje na bajtach są szybkie w procesorach

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Dziękuję za uwagę

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Podstawy kryptografii Wykład nr 3 Temat: Szyfrowanie asymetryczne

dr Michał Dolecki
Katedra Inteligencji Obliczeniowej
Zakład Uczenia Maszynowego

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

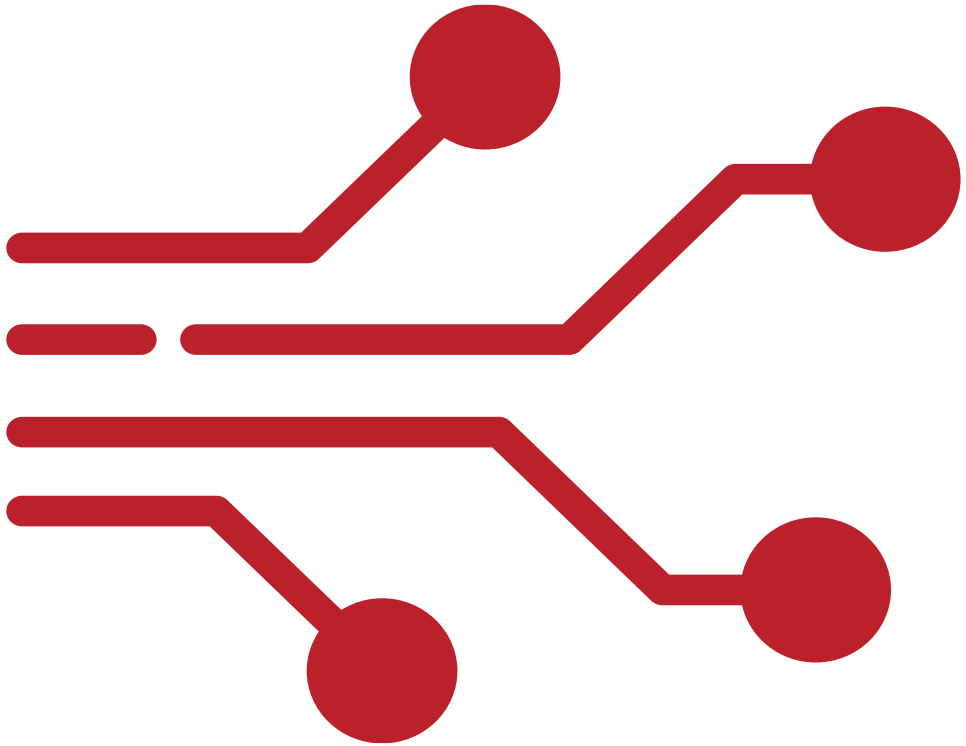
Plan wykładu

- Problemy kryptografii symetrycznej
- Kryptografia asymetryczna
- Rozszerzony algorytm Euklidesa
- Kryptosystem RSA

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

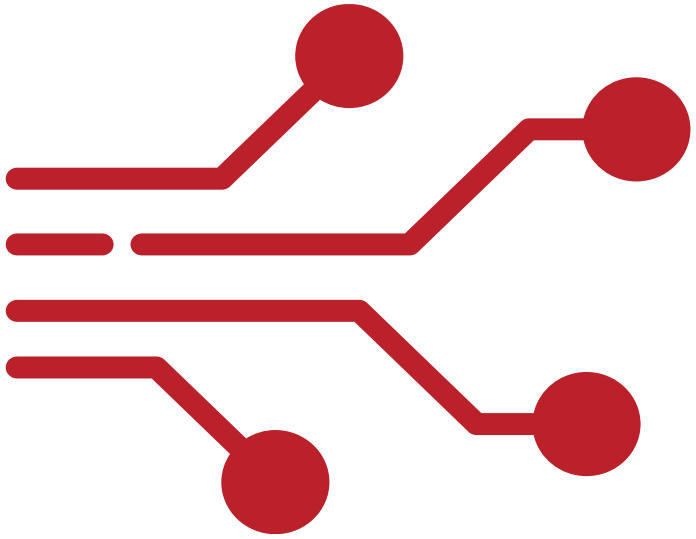
Problemy kryptografii symetrycznej



Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

3

Kryptografia symetryczna



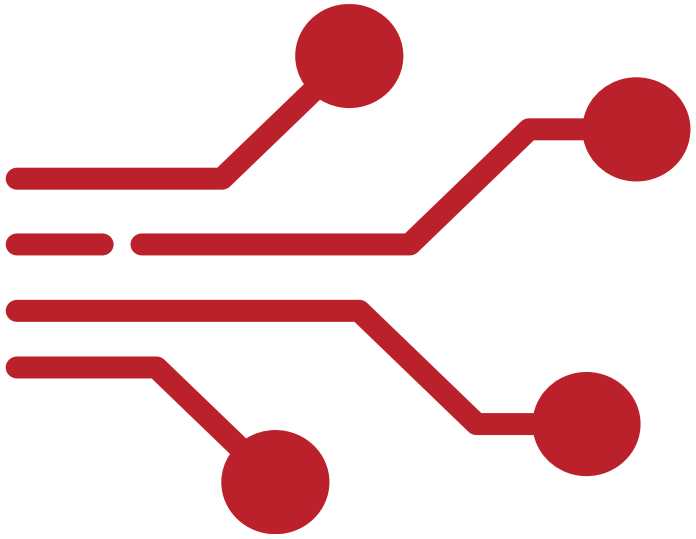
- **stosowana współcześnie**
- ważna historycznie
- obarczona jest ograniczeniami
  - problematyka zarządzania kluczami
  - skutki kompromitacji systemu
- poszukiwano alternatywnych rozwiązań

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

4

Problem przechowywania i dystrybucji kluczy



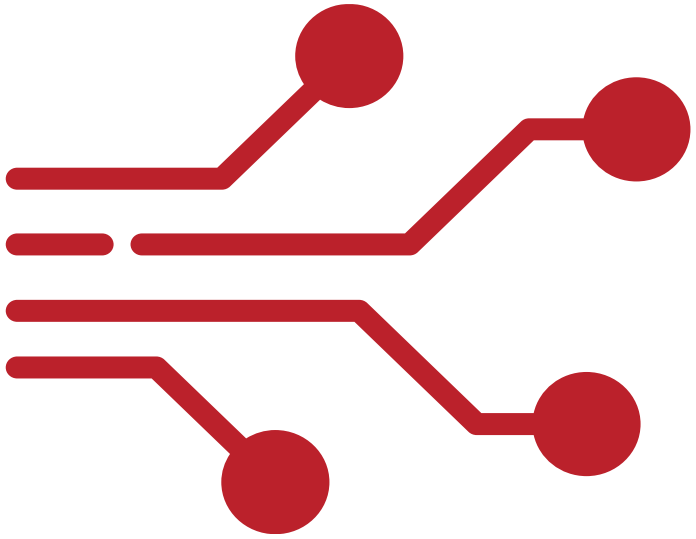
- założenie, że strony komunikujące się dysponują wspólnym, tajnym kluczem
- trudności natury praktycznej
- dla n użytkowników, gdzie każda para użytkowników pragnie prowadzić poufną komunikację
- każda para musi dysponować unikalnym, wspólnie współdzielonym kluczem

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

5

Liczba kluczy



Liczba niezbędnych kluczy K wyraża się wzorem:

$$K = \binom{n}{2} = \frac{n(n-1)}{2}$$

w sieci liczącej zaledwie 100 użytkowników, niezbędne staje się wygenerowanie, bezpieczne przechowanie i zarządzanie 4950 kluczami

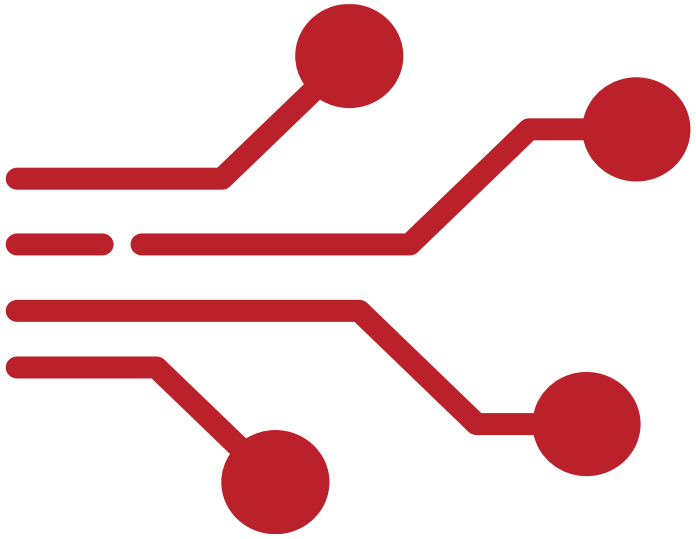
Wraz ze wzrostem n liczba kluczy rośnie kwadratowo

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

6

Dystrybucja kluczy



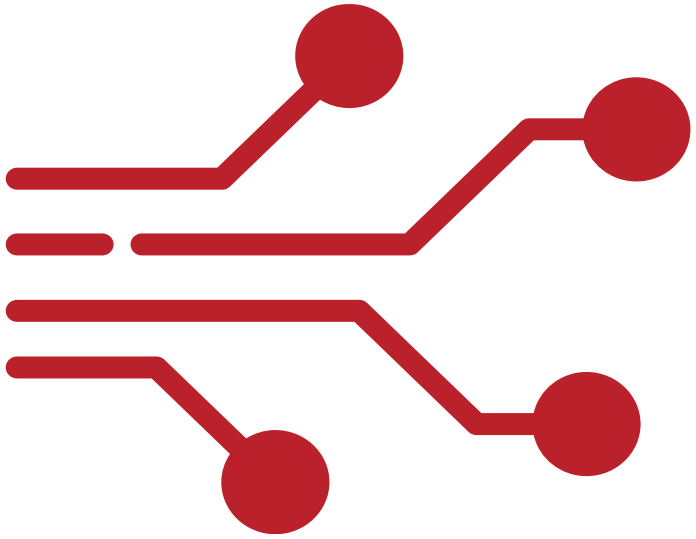
- Klucz symetryczny musi zostać przekazany stronom w sposób poufny i z autoryzacją
- wymaga to istnienia bezpiecznego kanału komunikacji, którego istnienie jest właśnie celem, a nie założeniem wstępnym

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

7

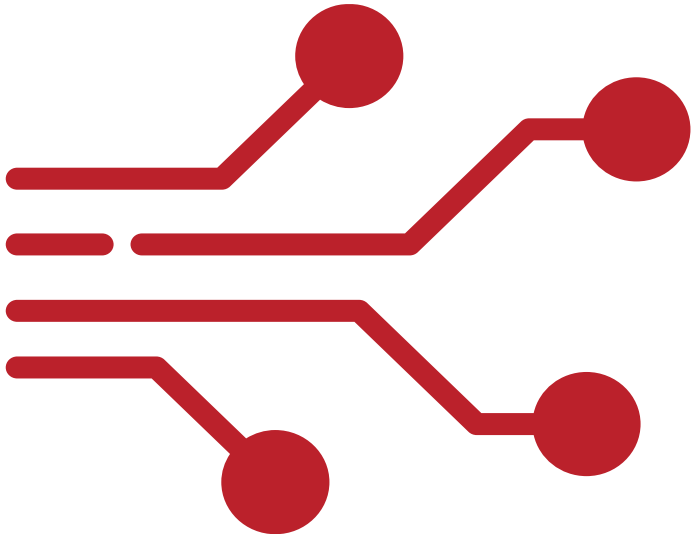
Atak na węzeł sieci



- każdy węzeł musi przechowywać wszystkie klucze do szyfrowania (swój i n-1 kluczy do komunikacji z pozostałymi węzłami)
- udany atak pozwala atakującemu przejąć wszystkie klucze

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Podsumowanie

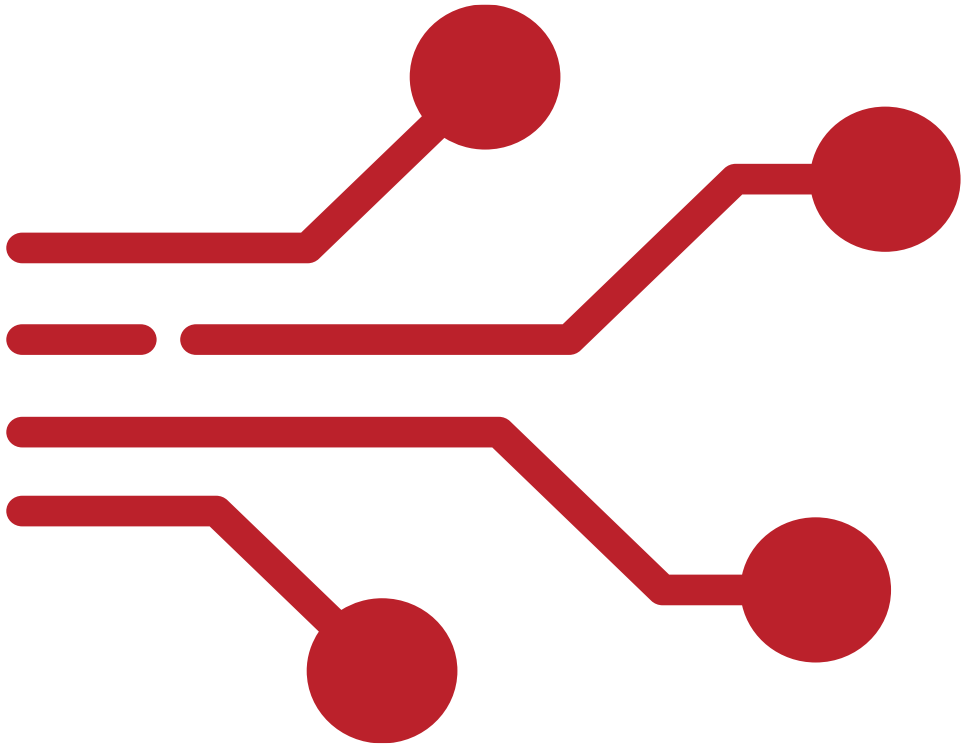


- kryptosystemy symetryczne cechuje skalowalność kwadratowa $O(n^2)$ w zakresie liczby kluczy
- W systemie asymetrycznym kompromitacja klucza prywatnego dotyczy wszystkich, którzy kiedykolwiek komunikowali się z danym użytkownikiem.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

9

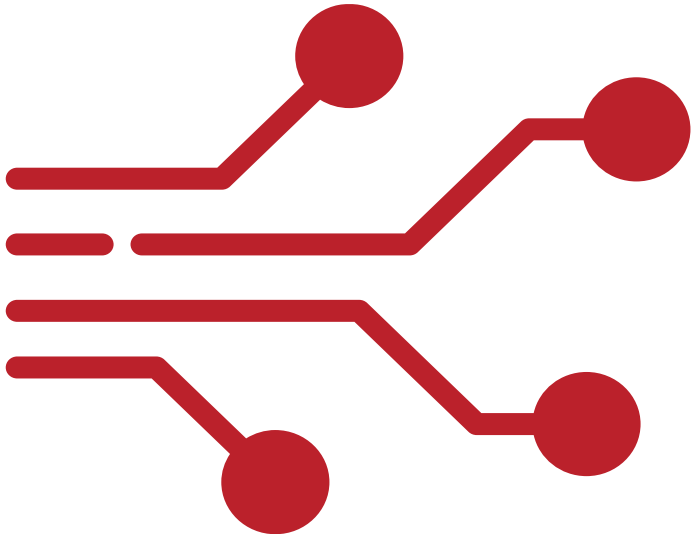
Kryptografia asymetryczna



Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

10

Zasada działania



Kryptografia asymetryczna

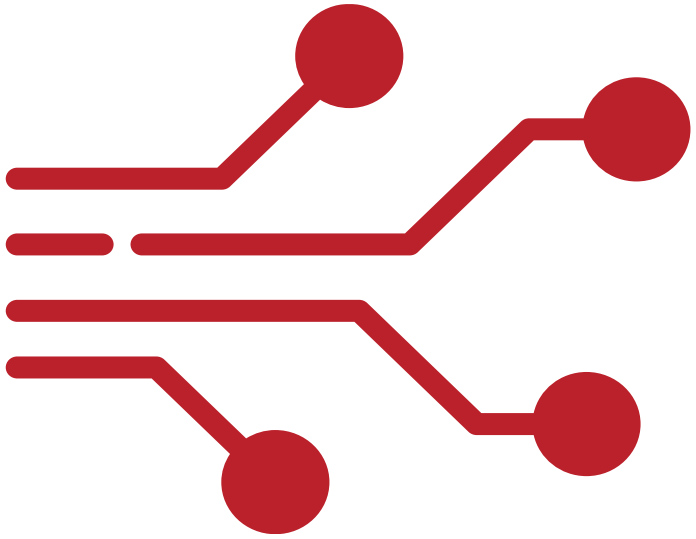
Kryptografia klucza publicznego

- Paradygmat odmienny od klasycznych systemów symetrycznych
- Paradygmat to przyjęty w danej dziedzinie wzorzec, model lub sposób widzenia rzeczywistości, działania i rozwiązywania problemów
- Zbiór podstawowych pojęć, teorii, metod i wartości, które uznaje większość ekspertów i na podstawie których formułuje się nowe teorie.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Zasada działania



Kryptografia asymetryczna opiera się na wykorzystaniu pary kluczy powiązanych ze sobą w taki sposób, że operacja odwrotna do szyfrowania jest praktycznie niewykonalna bez znajomości drugiego klucza pary.

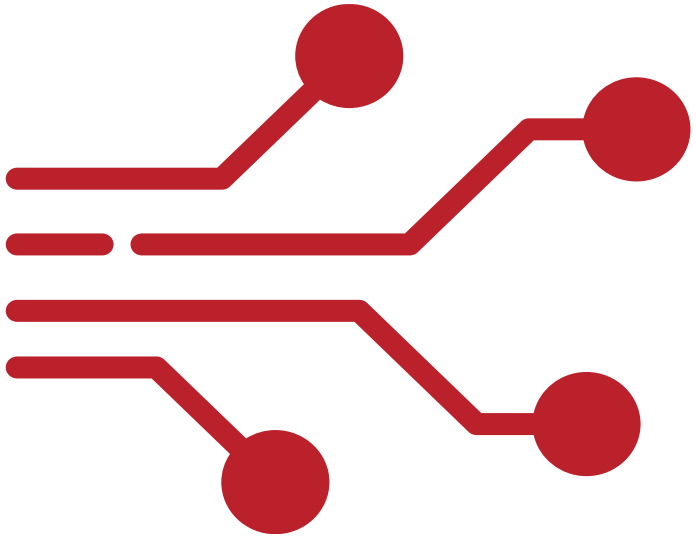
Znając jeden klucz z pary praktycznie nie możliwe jest wyznaczenie drugiego klucza.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

12

Formalna struktura kryptosystemu



- system kryptografii asymetrycznej definiuje się jako piątkę

$$(P, C, K, E, D)$$

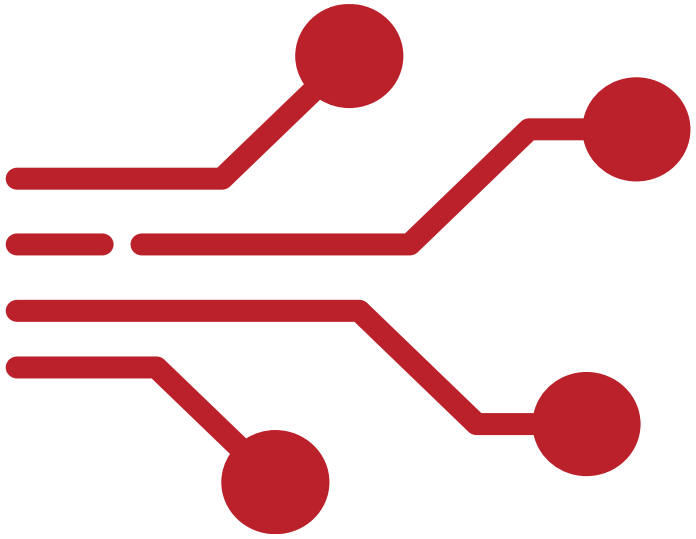
- P oznacza przestrzeń tekstów jawnych (wiadomości),
- C oznacza przestrzeń szyfrogramów,
- K oznacza przestrzeń kluczy,
- $E\ i\ D$ oznaczają funkcje szyfrującą i deszyfrującą

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

13

Porównanie z kryptografią symetryczną



- Kluczową różnicą w stosunku do kryptografii symetrycznej jest struktura przestrzeni kluczy
- Każdy użytkownik U dysponuje parą kluczy

$$(pk, sk) \in K_{pub} \times K_{priv},$$

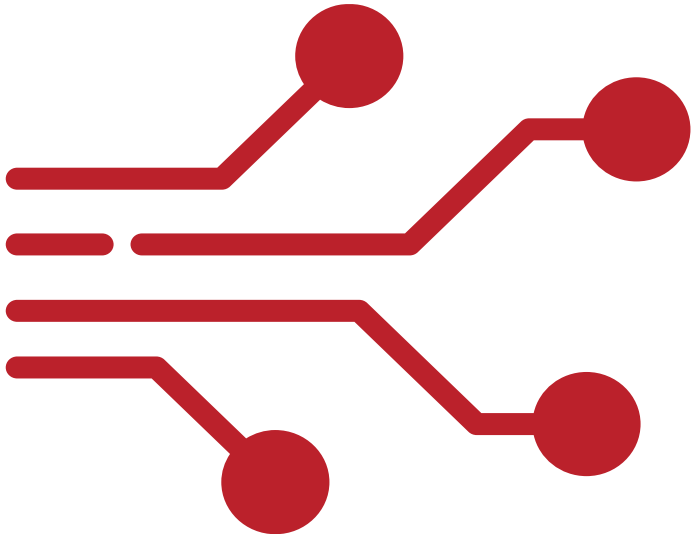
- gdzie:
  - pk – klucz publiczny
  - sk – klucz prywatny

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

14

Warunki działania kryptosystemu



- Dla każdej pary (pk, sk) istnieją odwzorowania:
$$E_{pk}: P \to C, D_{sk}: C \to P$$

- spełniające warunek **poprawności**:
$$\forall m \in P: D_{sk}(E_{pk}(m)) = m$$

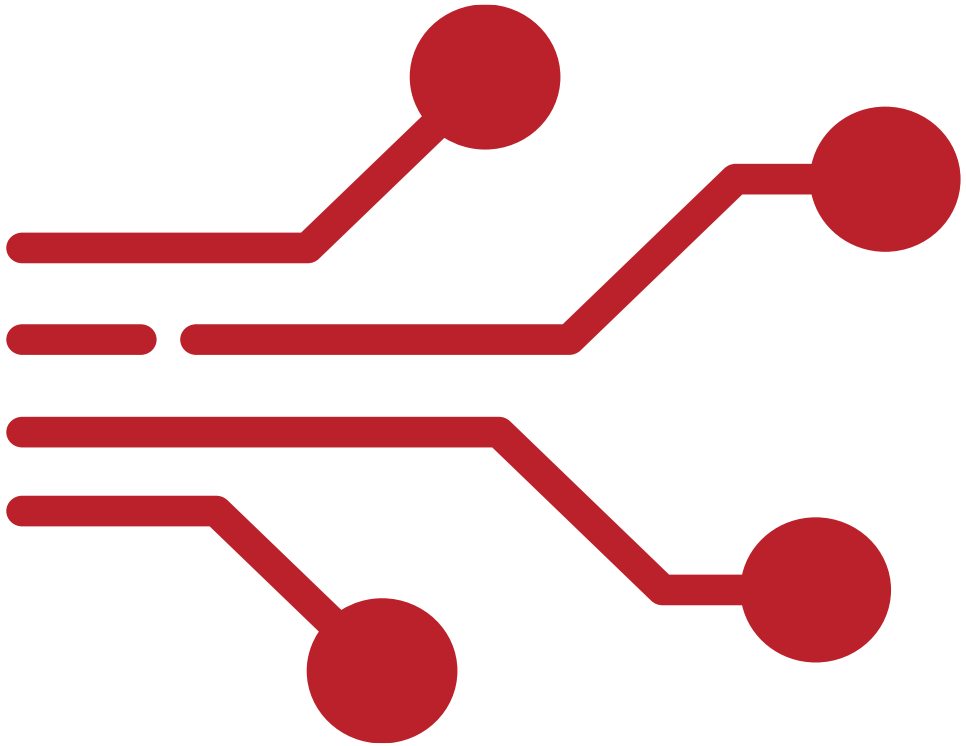
- oraz warunek **bezpieczeństwa**: znając pk oraz $c = E_{pk}(m)$, obliczenie m bez znajomości sk jest obliczeniowo niewykonalne.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

15

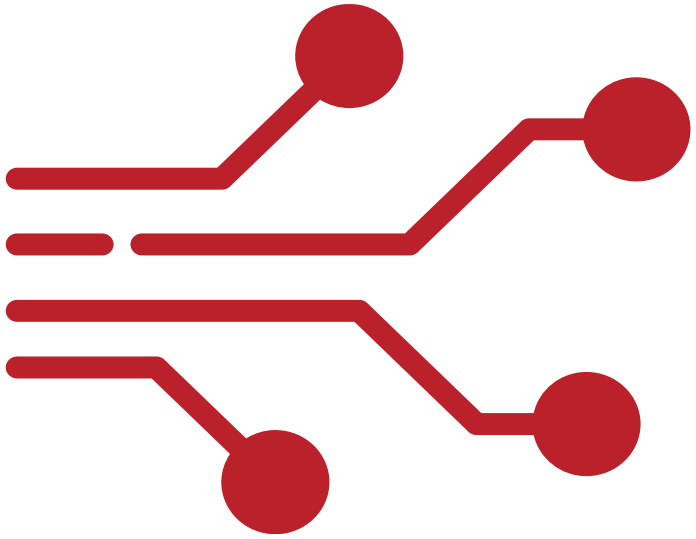
Algorytm Euklidesa



Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

16

Wprowadzenie



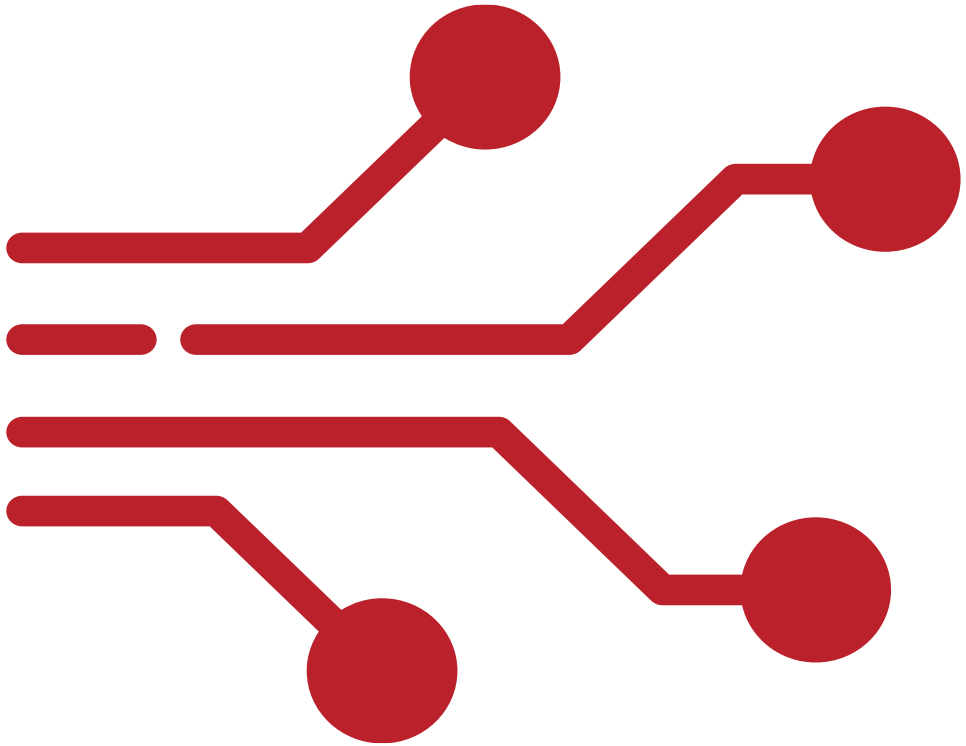
- jest jedną z najstarszych i najbardziej fundamentalnych procedur obliczeniowych w teorii liczb.
- Służy do wyznaczania największego wspólnego dzielnika dwóch liczb całkowitych.
- Przedstawimy jego podstawową wersję oraz rozszerzenie niezbędne w kontekście kryptografii asymetrycznej.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

17

Kryptosystem RSA

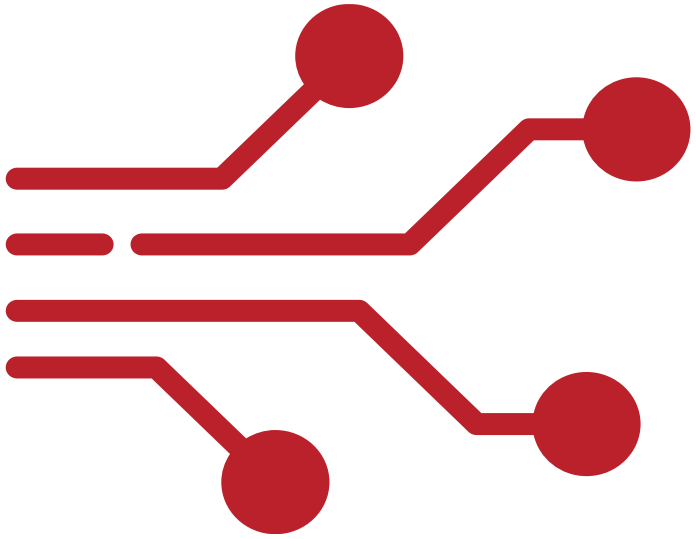


Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

18

Kryptosystem RSA



- Jeden z najstarszych kryptosystemów asymetrycznych
- Szeroko stosowany do bezpiecznej transmisji danych
  - wymiany informacji poprzez kanały o niskiej poufności,
  - w systemach elektronicznego uwierzytelniania,
  - obsługi podpisów cyfrowych,
  - do szyfrowania poczty,
  - itd.
- Akronim "RSA" pochodzi od nazwisk
  - Rona Rivesta,
  - Adiego Shamira,
  - Leonarda Adlemana,

  którzy publicznie opisali ten algorytm w 1977

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Twórcy RSA

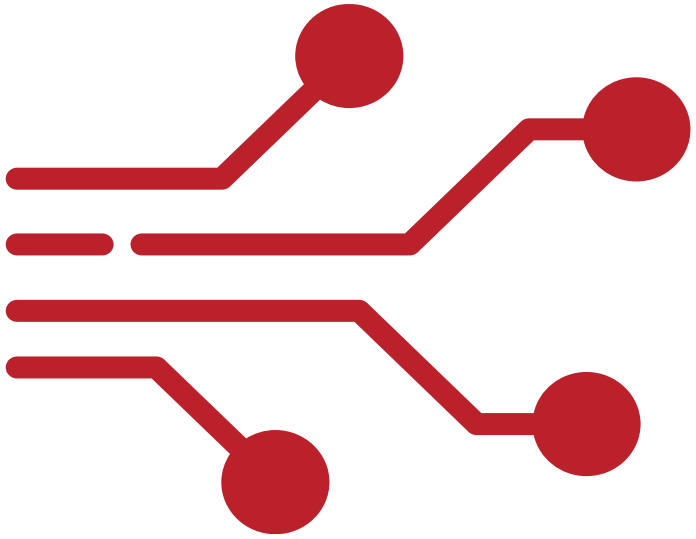
20

https://www.abc.net.au/news/science/2018-01-20/how-prime-numbers-rsa-encryption-works/9338876

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Problem faktoryzacji

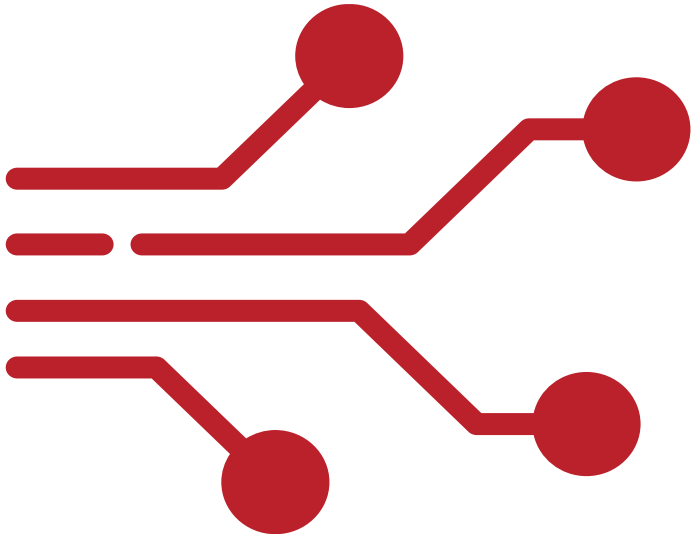


- Bezpieczeństwo RSA jest związane z trudnością faktoryzacji dużej liczby złożonej.
  - 21 = 3 * 7
  - 988027 = ?
  - liczba o 2048 bitach = ???
- Moduł powstaje z iloczynu dwóch dużych liczb pierwszych.
- Złamanie szyfrowania RSA znane jest jako problem RSA.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Historia RSA



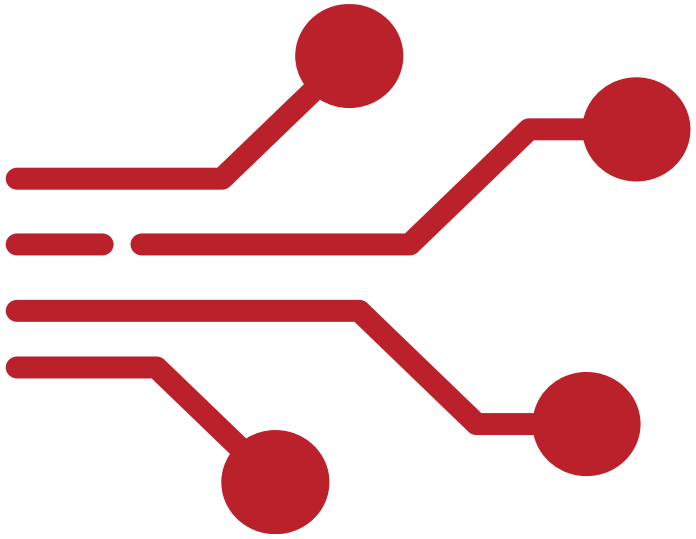
- W 1976 roku Whitfield Diffie i Martin Hellman opublikowali artykuł przedstawiający możliwość stworzenia algorytmu szyfrującego używającego jednego klucza do zaszyfrowywania informacji, a drugiego do odszyfrowywania.
- Na ten sam pomysł wpadł Robert Merkle, ale jego praca na ten temat ukazała się, gdy idea kryptografii bazującej na kluczu publicznym była już znana.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

22

Wcześniejsze prace



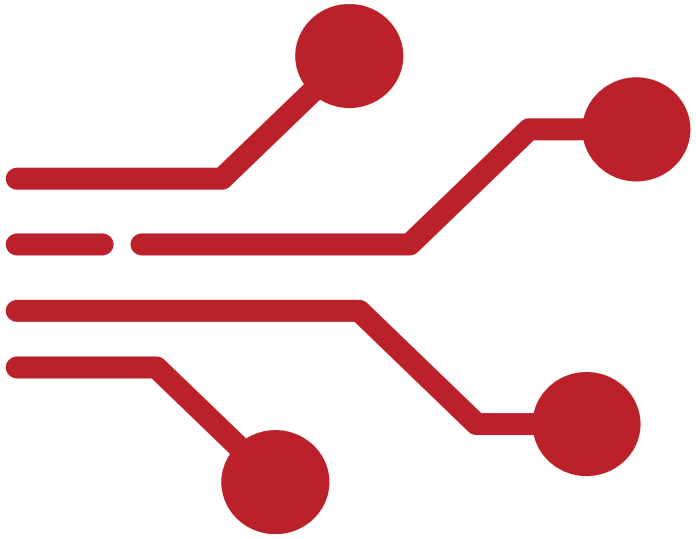
- Idea kryptografii asymetrycznej prawdopodobnie była znana wcześniej tajnym służbom
- Równoważny system został opracowany w tajemnicy w 1973 roku w brytyjskiej agencji wywiadu, przez angielskiego matematyka Clifforda Cocksa. System ten został odtajniony w 1997 roku

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

23

Szyfrowanie



- Nadawca pobiera klucz publiczny odbiorcy (n, e).
- Wiadomość zostaje zamieniona na liczbę naturalną m, o własności: 0 < m < n.
- Odbiorca musi znać użyty sposób przekształcenia tekstu w liczbę, aby mógł później odtworzyć otrzymaną wiadomość.
- Wykonując operację szyfrowania oblicza się:

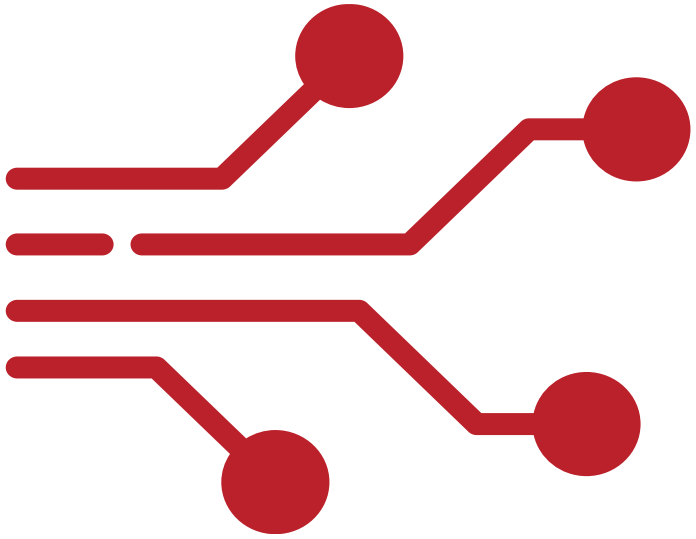
$$c = m^e \bmod n$$

- Liczba c jest zaszyfrowaną wiadomością i jest ona przekazywana odbiorcy.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Deszyfrowanie



- Odbiorca od nadawcy otrzymuje zaszyfrowaną wiadomość w postaci liczby naturalnej, która spełnia warunek 0 < c < n.
- Liczba c jest przekształcana na pierwotną wartość m stosując wzór:

$$m = c^d \, mod \, n.$$

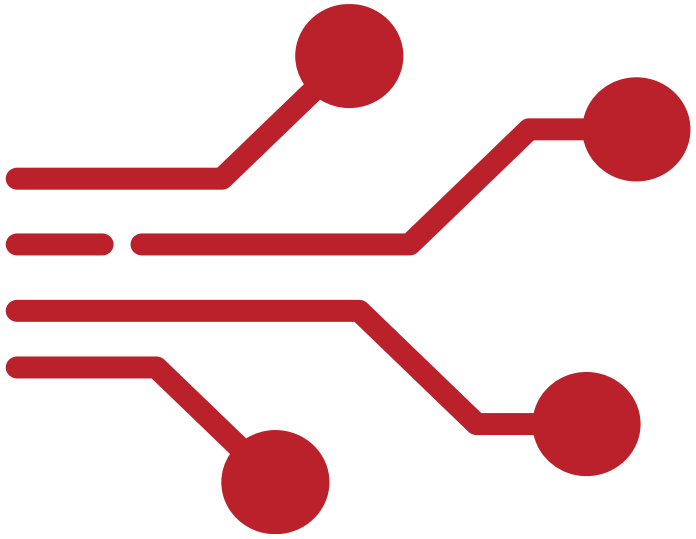
- Z otrzymanej liczby c odbiorca odtwarza tekst i odczytuje przesłaną wiadomość.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

25

Podsumowanie



- Szyfrowanie

$$c = m^e \bmod n$$

- Deszyfrowanie

$$m = c^d \bmod n$$

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

26

Przykład

- Klucze odbiorcy (n,e)=(33,13) oraz (n,d)=(33,17).
- Wiadomość u nadawcy m=15.

$$c = m^e \text{ mod } n = 15^{13} mod\ 33 = 9$$

- Zatem c=9 jest zaszyfrowaną wiadomością.

- Odbiorca otrzymał zaszyfrowaną wiadomość c=9.

$$m = c^d\ mod\ n = 9^{17} mod\ 33 = 15$$

- Odbiorca otrzymał wiadomość m=15.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

27

Uzasadnienie działania RSA

$$D\big(E(m)\big) = m$$

Nie jest to pełny dowód, a jedynie ogólny zarys obliczeń pokazujących dlaczego szyfrowanie i deszyfrowanie działają

$$E(m) = m^e \bmod n = c$$

$$D(c) = c^d \bmod n = \big(m^e\big)^d \bmod n = m^{ed} \bmod n$$

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

28

Dziękuję za uwagę

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Podstawy kryptografii
Wykład nr 4
Temat: Podpisy Cyfrowe

Dr inż. Marek B.Horyński
Katedra Informatyki Stosowanej

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Plan prezentacji

Plan wykładu

- Wprowadzenie: Problem Zaufania
- Podstawy Kryptograficzne
- Anatomia Podpisu Cyfrowego
- Infrastruktura Klucza Publicznego (PKI)
- Zastosowania i Kontekst Prawny
- Wyzwania i Przyszłość

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Temat

Problem Zaufania w Świecie Cyfrowym

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

3

Podstawy: Funkcje Skrótu (Hashing)

Koncepcja: "Cyfrowy Odcisk Palca"

Funkcja skrótu (np. SHA-256) przekształca dowolną ilość danych w unikalny ciąg znaków o stałej długości (skrót).

- **Jednokierunkowa:** Niemożliwe jest odtworzenie danych wejściowych na podstawie skrótu.
- **Deterministyczna:** Te same dane wejściowe zawsze dają ten sam skrót.
- **Odporna na kolizje:** Niezwykle trudne jest znalezienie dwóch różnych wejść dających ten sam skrót.
- **Kluczowa dla zapewnienia INTEGRALNOŚCI.**

Odcisk palca Stockowa ilustracja wektorowa (iStock by Getty Images)

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Podstawy: Dwa Modele Kryptografii

Kryptografia Symetryczna

Jeden, tajny klucz jest używany do szyfrowania i deszyfrowania.

Szybka, idealna do dużych danych, ale... jak bezpiecznie przekazać klucz?

Kryptografia Asymetryczna

Para matematycznie powiązanych kluczy:

Prywatny (tajny) i **Publiczny** (jawny).

Rozwiązuje problem dystrybucji kluczy.

Fundament podpisów cyfrowych.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Proces Podpisywania (Perspektywa Nadawcy)

Anatomia Podpisu Cyfrowego

Krok 1: Dokument

Oryginalna wiadomość lub plik do podpisania.

Krok 2: Skrót

Dokument jest przetwarzany przez funkcję skrótu (np. SHA-256).

Krok 3: Szyfrowanie

Skrót jest szyfrowany za pomocą klucza prywatnego nadawcy.

Wynik: Podpis

Zaszyfrowany skrót to jest właśnie Podpis Cyfrowy.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Proces Weryfikacji (Perspektywa Odbiorcy)

Odbiorca otrzymuje: [Oryginalny Dokument] + [Podpis Cyfrowy] + [Klucz Publiczny Nadawcy]

Ścieżka A: Weryfikacja Podpisu

1. Odbiorca deszyfruje [Podpis Cyfrowy] używając **klucza publicznego** nadawcy.
2. Wynik: **Oryginalny Skrót (A)**.

Ścieżka B: Obliczenie Własne

1. Odbiorca niezależnie przepuszcza [Oryginalny Dokument] przez tę samą funkcję skrótu.
2. Wynik: **Nowy Skrót (B)**.

Werdykt: Czy Skrót (A) == Skrót (B)?

TAK: Podpis autentyczny, dokument nienaruszony.

NIE: Podpis nieważny lub dokument został zmieniony.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Kluczowa Różnica: Podpis vs. Szyfrowanie

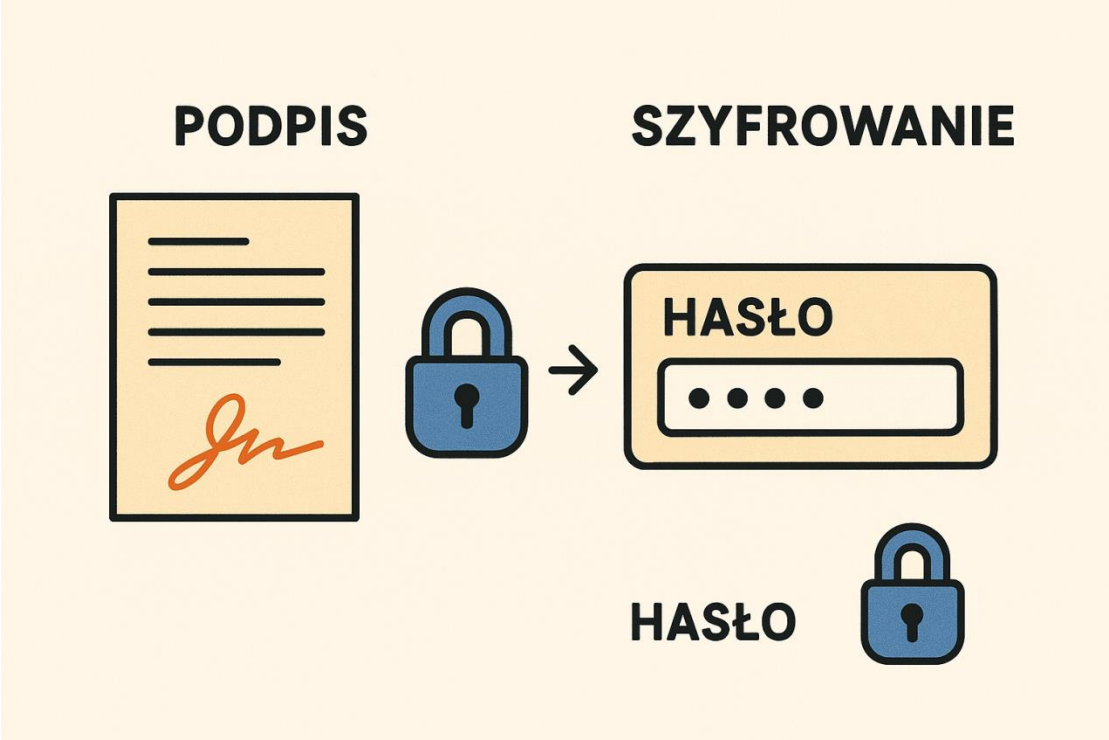
Podpis Cyfrowy (Klucz Prywatny)

Zapewnia autentyczność, integralność i niezaprzeczalność. **Nie ukrywa treści dokumentu**. Odpowiada na pytanie: "Kto to podpisał i czy nic się nie zmieniło?".

Szyfrowanie (Klucz Publiczny)

Zapewnia poufność. **Ukrywa treść dokumentu**. Odpowiada na pytanie: "Czy ta wiadomość jest tylko dla mnie?".

Oba procesy są od siebie niezależne, ale często stosowane razem (np. w S/MIME).



Opracowanie własne na podstawie dokumentów eiDAS

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Gwarancje Podpisu Cyfrowego

Autentyczność

Tylko właściciel klucza prywatnego mógł wygenerować ten podpis. Mamy pewność co do tożsamości nadawcy.

Integralność

Weryfikacja skrótu gwarantuje, że dokument nie został zmieniony ani o jeden bit od momentu podpisania.

Niezaprzeczalność

Nadawca nie może się wyprzeć faktu podpisania dokumentu, ponieważ tylko on ma kontrolę nad swoim kluczem prywatnym.

Opracowanie własne na podstawie dokumentów eiDAS

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Problem Zaufania i Urzędy Certyfikacji (CA)

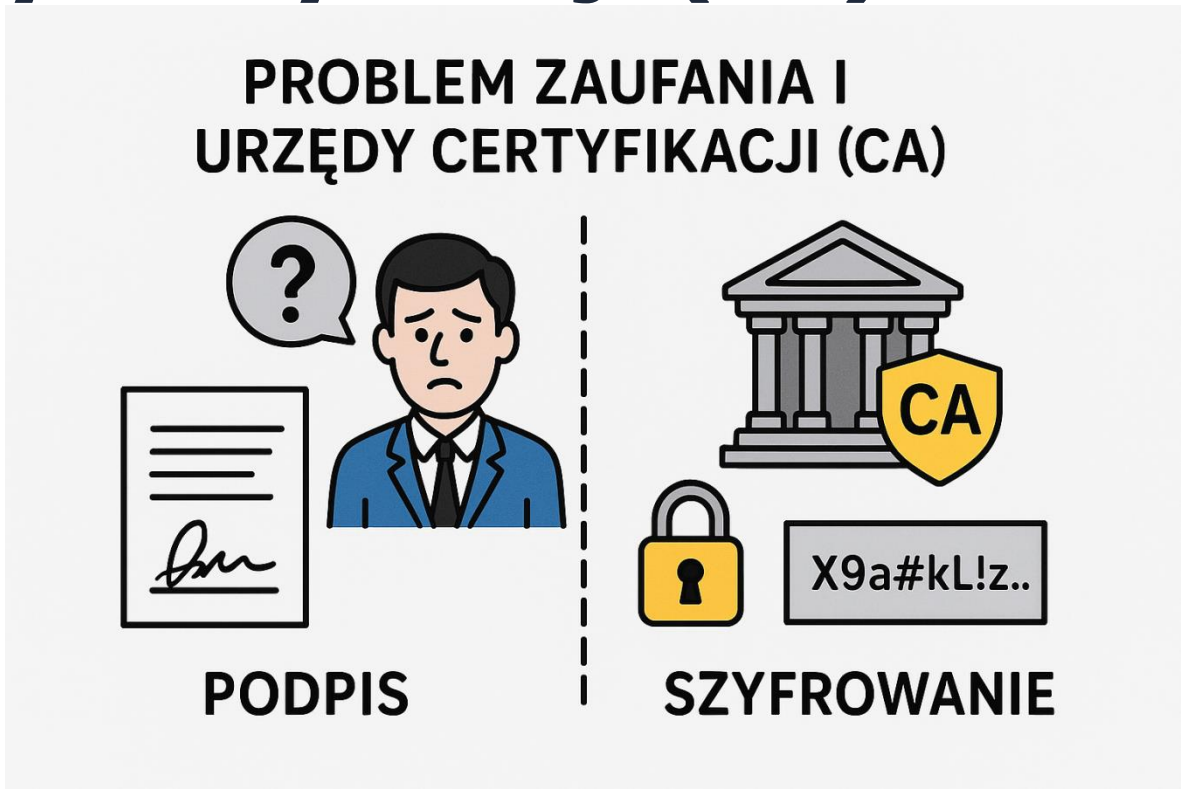
Problem: Skąd mam wiedzieć?

Otrzymałem klucz publiczny od "Banku". Ale skąd mam pewność, że ten klucz *naprawdę* należy do Banku, a nie do atakującego (Man-in-the-Middle)?

Rozwiązanie: Zaufana Strona Trzecia

Urząd Certyfikacji (CA) działa jak "cyfrowy notariusz":

- Weryfikuje tożsamość podmiotu (np. Banku).
- Wydaje **Certyfikat Cyfrowy**, który zawiera klucz publiczny Banku i jest *podpisany cyfrowo przez CA*.
- My ufamy CA, więc możemy ufać kluczowi publicznemu w certyfikacie.



Opracowanie własne na podstawie dokumentów eiDAS

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Standard: Certyfikat Cyfrowy X.509

Certyfikat cyfrowy to standardowa struktura danych (X.509), która publicznie wiąże tożsamość z kluczem publicznym. Zawiera m.in.:

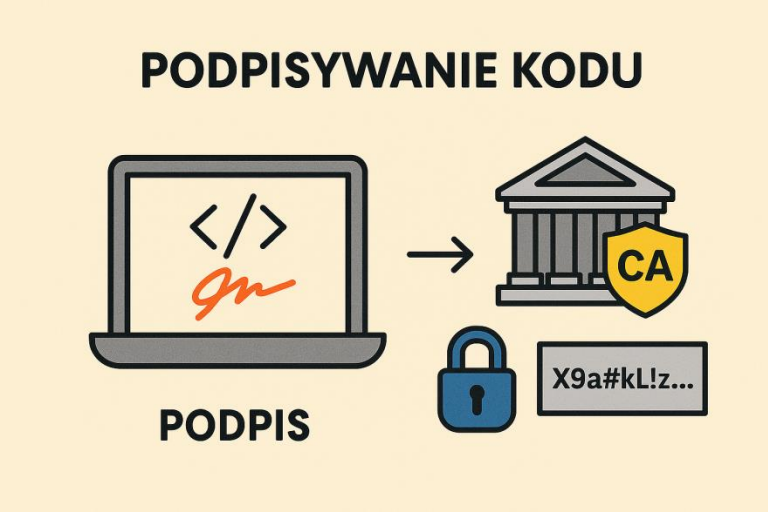
- **Właściciel (Subject):** Do kogo należy certyfikat (np. `google.com`).
- **Klucz Publiczny Właściciela:** Klucz, który jest certyfikowany.
- **Wystawca (Issuer):** Który Urząd Certyfikacji (CA) to wydał.
- **Podpis Cyfrowy Wystawcy:** Podpis CA gwarantujący autentyczność certyfikatu.
- **Okres Ważności:** Kiedy certyfikat jest ważny.

Opracowanie własne na podstawie dokumentów eiDAS

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Zastosowania w Praktyce



Podpisywanie Kodu (Code Signing)

Gwarantuje, że oprogramowanie pochodzi od autoryzowanego wydawcy i nie zostało zmodyfikowane.

Bezpieczna Poczta (S/MIME, PGP)

Uwierzytelnienie nadawcy wiadomości e-mail oraz zapewnienie integralności jej treści.

Dokumenty Elektroniczne (PDF, PAdES)

Prawnie wiążące umowy, e-faktury, dokumenty urzędowe (np. w systemie ePUAP).

Opracowanie własne na podstawie dokumentów eiDAS

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Kontekst Prawny w UE: Rozporządzenie eIDAS

Na podstawie dokumentów eiDAS

eIDAS standaryzuje podpisy w UE:

- **Zwykły podpis (SES):** Np. skan podpisu, kliknięcie "Zgadzam się". Niska moc dowodowa.
- **Zaawansowany podpis (AdES):** Unikalnie powiązany z podpisującym, pozwala na identyfikację, oparty na certyfikacie.
- **Kwalifikowany podpis (QES):** Najwyższy poziom. Tworzony za pomocą kwalifikowanego urządzenia (np. token, karta), oparty na kwalifikowanym certyfikacie. **Ma moc prawną równoważną podpisowi odręcznemu w całej UE.**

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Wyzwanie: Zagrożenie Kwantowe

Problem: Algorytm Shora

Obecna kryptografia asymetryczna (RSA, ECC) opiera swoją siłę na trudności matematycznej faktoryzacji dużych liczb pierwszych.

Problem ten jest trywialny do rozwiązania dla wystarczająco potężnych komputerów kwantowych (używających algorytmu Shora).

Oznacza to, że w przyszłości komputery kwantowe będą w stanie złamać każdy obecny klucz prywatny na podstawie publicznego, czyniąc obecne podpisy bezużytecznymi.

Wizualizacja komputera kwantowego [14]

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Rozwiązanie: Kryptografia Postkwantowa (PQC)

Nowe Fundamenty Matematyczne

Kryptografia Postkwantowa (PQC) to algorytmy odporne na ataki zarówno komputerów klasycznych, jak i kwantowych.

Bazują na innych problemach (np. kryptografia oparta na sieciach krystalicznych, hashowaniu, kodowaniu).

Wyzwanie: Migracja

Trwa globalny wyścig (kierowany np. przez NIST) w celu standaryzacji i wdrożenia algorytmów PQC.

Największym wyzwaniem będzie masowa migracja globalnej infrastruktury IT zanim komputery kwantowe staną się realnym zagrożeniem.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Bibliografia

I. Literatura Akademicka (Kryptografia i PKI)

1. Menezes, A. J., van Oorschot, P. C., Vanstone, S. A. (2005). Kryptografia Stosowana. Warszawa: Wydawnictwa Naukowo-Techniczne (WNT). (lub późniejsze wydania).

Komentarz: Kluczowa pozycja akademicka, wyczerpująco opisująca algorytmy klucza publicznego, funkcje skrótu oraz protokoły podpisu cyfrowego, stanowiąca fundament wiedzy o kryptografii.

2. Kościelny, C., Kurkowski, M., Srebrny, M. (2009). Kryptografia. Teoretyczne podstawy i praktyczne zastosowania. Warszawa: Wydawnictwo PJATK.

Komentarz: Przystępny podręcznik opisujący podstawy kryptografii symetrycznej i asymetrycznej oraz ich zastosowania w sieciach komputerowych, w tym PKI.

II. Źródła Prawne (Kontekst Europejski)

3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (eIDAS).

Komentarz: Podstawowy akt prawny regulujący definicje, rodzaje (zaawansowany, kwalifikowany) i skutki prawne podpisów elektronicznych w UE.

4. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

Komentarz: Polski akt wdrażający i uzupełniający przepisy Rozporządzenia eIDAS w krajowym porządku prawnym.

III. Standardy i Wyzwania Przyszłości (Kryptografia Postkwantowa)

5. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization.

Komentarz: Oficjalna strona internetowa projektu standaryzacji algorytmów PQC. Należy cytować konkretne standardy (np. FIPS 204: ML-DSA), gdy zostaną opublikowane.

6. FIPS 204 (Federal Information Processing Standards Publication 204). Module-Lattice-Based Digital Signature Algorithm (ML-DSA) (Oczekiwane lub opublikowane wydanie).

Komentarz: Standard NIST określający algorytm postkwantowego podpisu cyfrowego (wcześniej znany jako CRYSTALS-Dilithium), kluczowy w kontekście przyszłej migracji.

7. Cooper, D., et al. (2008). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Zakończenie

Dziękuję za uwagę

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Podstawy kryptografii
Wykład nr 5

Temat: Steganografia
Sztuka Ukrywania Komunikacji w Świecie Cyfrowym

Dr inż. Marek B.Horyński
Katedra Informatyki Stosowanej

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Plan prezentacji

- Wprowadzenie: Pojęcie steganografii
- Steganografia vs. Kryptografia
- Główne Nośniki Informacji Cyfrowej
- Rewolucja Cyfrowa i Nadmiarowość Danych
- Główne Nośniki Informacji Cyfrowej
- LSB: Ukrywanie w Najmniej Znaczącym Bicie
- Główne Metody Steganografii Obrazu
- Steganografia Audio i Wideo
- Steganografia Tekstowa: Ukryte Wzorce
- Steganografia Sieciowa (Protokół)
- Klucze i Zasada Kerckhoffsa
- Legalne Zastosowanie: Cyfrowe Znaki Wodne
- Uwierzytelnianie i Autentyczność Dokumentów
- Ciemna Strona: Ukrywanie Złośliwego Kodu
- Steganaliza: Rozpoznanie i Wykrywanie
- Kluczowe Metody Steganalizy
- Przyszłość: Kierunki Rozwoju

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

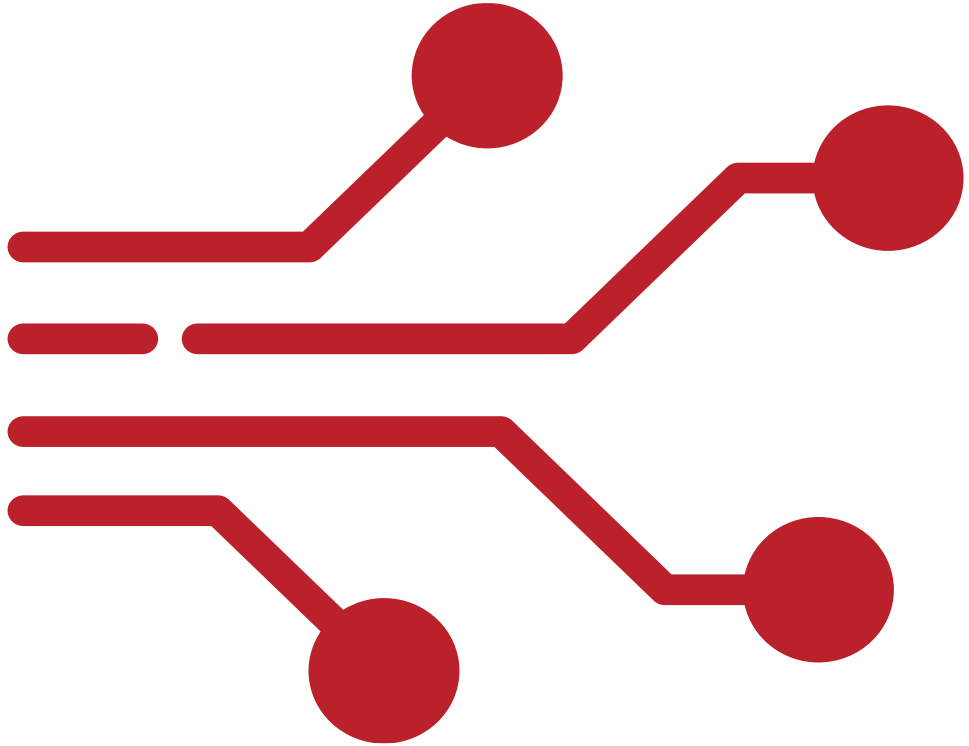
Co to jest Steganografia?

Greckie korzenie ("ukryte pismo"). Nauka i praktyka ukrywania wiadomości, obrazu lub pliku w innym nośniku w taki sposób, że sama obecność ukrytej informacji jest niewidoczna

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Steganografia vs. Kryptografia



Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

4

Steganografia vs. Kryptografia

Kryptografia

Ukrywa **treść** wiadomości poprzez jej zaszyfrowanie. Fakt komunikacji jest **znany** i widoczny (zaszyfrowany plik/tekst). Używa algorytmów i kluczy.

Steganografia

Ukrywa **fakt istnienia** wiadomości wewnątrz niewinnego nośnika (np. obrazu, audio). Wiadomość jest **niewidoczna** dla osób trzecich. Kluczowy cel to uniknięcie podejrzeń.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

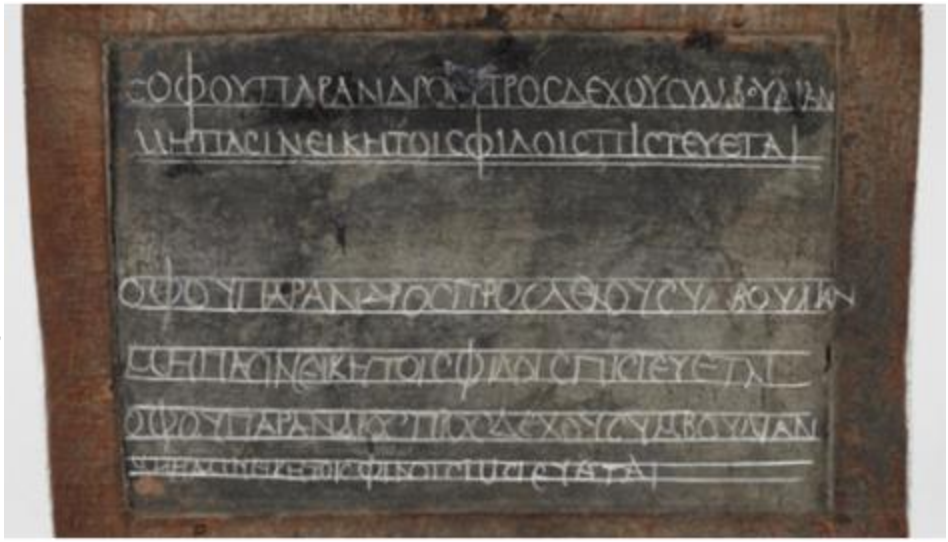
Historia: Od Herodota do Mikrokropki

Przykłady historyczne:

Tatuaże na głowach: W starożytnej Grecji wiadomości tatuowano na ogolonych głowach niewolników, a następnie ukrywano pod odrastającymi włosami.

Ukryte pismo na tabliczkach woskowych: Wiadomość ryto w drewnie, które następnie pokrywano woskiem i wykorzystywano do "zwykłych" notatek.

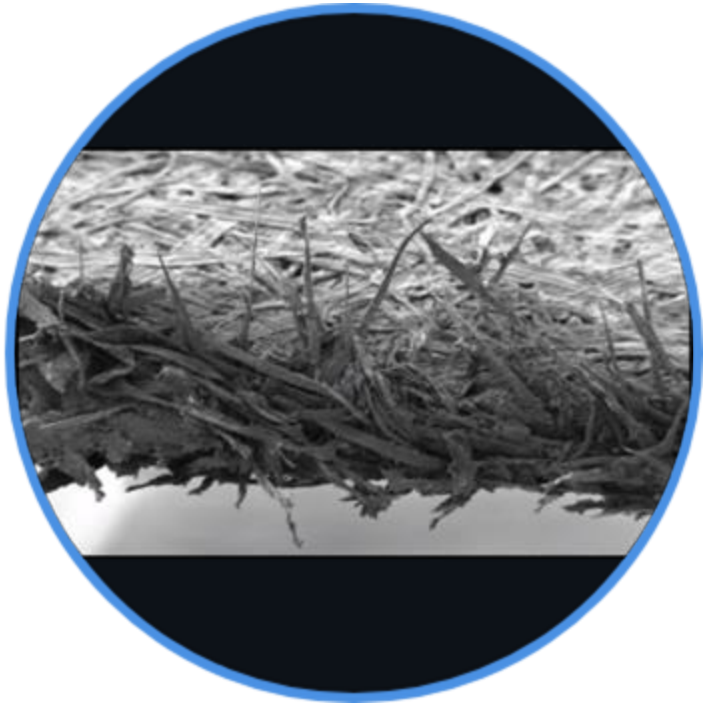
Tajnopis (niewidzialny atrament): Użycie cieczy, która stawała się widoczna dopiero po podgrzaniu lub naświetleniu.



Źródło: www.bl.uk

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską



Źródło: www.reddit.com

Technika II Wojny Światowej

Mikrokropka była zdjęciem o wysokiej rozdzielczości, pomniejszonym do rozmiaru kropki w tekście maszynopisu lub na kartce pocztowej.

Używana głównie przez szpiegów, ponieważ pozwalała na przesyłanie obszernej, tajnej informacji bez wzbudzania najmniejszych podejrzeń o istnieniu jakiejkolwiek komunikacji.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Rewolucja Cyfrowa i Nadmiarowość Danych

W cyfrowej steganografii nośnikiem (kontenerem) jest plik komputerowy. Pliki multimedialne są idealne ze względu na ich naturalną nadmiarowość – małe zmiany są niezauważalne dla ludzkiej percepcji.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Główne Nośniki Informacji Cyfrowej

Najczęściej używany nośnik (JPEG, PNG). Posiada ogromną ilość pikseli do ukrycia danych.

Fale dźwiękowe i ich binarna sekwencja (MP3, WAV). Trudniejsze ze względu na czułość słuchu.

Ukrywanie w strumieniu ruchomych obrazów i dźwięków (MP4, AVI). Pozwala na ukrycie dużej ilości danych.

Modyfikacja białych znaków, kodowania lub nagłówków pakietów sieciowych (TCP/IP).

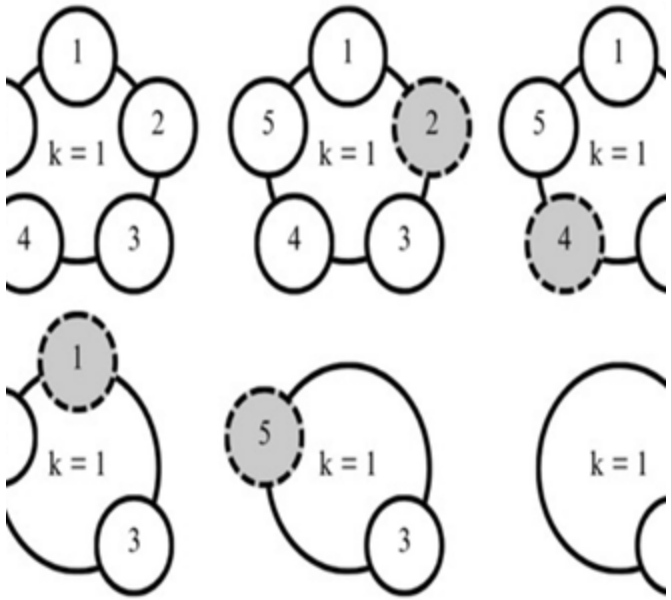
Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

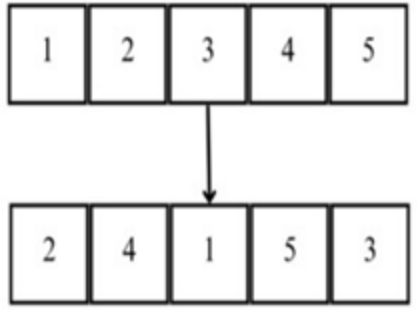
LSB: Ukrywanie w Najmniej Znaczącym Bicie

Mechanizm LSB

Najpopularniejsza technika w steganografii cyfrowej. Polega na modyfikacji najmniej znaczącego bitu (LSB) każdego piksela w obrazie lub każdej próbki w pliku audio.

Zastąpienie LSB ukrytą informacją zmienia wartość koloru (lub dźwięku) tylko minimalnie, co jest **wizualnie i akustycznie niezauważalne** dla człowieka. Zmiana jest równoznaczna z +/- 1 w skali od 0 do 255.





Źródło: https://www.mdpi.com/applsci/applsci-14-07119/article_deploy/html/images/applsci-14-07119-g001-550.jpg

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Główne Metody Steganografii Obrazu

Domena Przestrzenna (Spatial Domain)

Najprostsze metody, takie jak LSB (Least Significant Bit), gdzie dane są osadzane bezpośrednio w wartościach pikseli.

Domena Częstotliwości (Frequency Domain)

Wykorzystanie transformacji, np. Transformata Kosinusowa (DCT - JPEG) lub Transformata Fouriera, do ukrycia danych w współczynnikach częstotliwości obrazu, co jest bardziej odporne na kompresję.

Adaptacyjne Ukrywanie

Osadzanie informacji w regionach obrazu, które mają naturalnie wyższą złożoność (szum), co dodatkowo utrudnia wykrycie statystyczne.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Steganografia Audio i Wideo

Audio (Dźwięk)

Polega na osadzeniu tajnych wiadomości w sygnale audio poprzez modyfikację sekwencji binarnej pliku. Wykorzystuje się:

- LSB w próbkach audio.
- Maskowanie spektralne (wykorzystanie słabiej słyszalnych częstotliwości).

Źródło: implex.dev

Wideo (Obraz Ruchomy)

Osadzanie danych w cyfrowych formatach wideo. Pozwala na ukrycie dużych ilości danych.

- Ukrywanie w nieskompresowanym wideo.
- Osadzanie w skompresowanym strumieniu danych (np. w klatkach I, P lub B).

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Steganografia Tekstowa: Ukryte Wzorce

Źródło: forum.cursor.com

Modyfikacje Niewidoczne

Polega na ukrywaniu informacji wewnątrz plików tekstowych lub kodu źródłowego.

- **Ukrywanie w białych znakach:** Zmiana układu spacji lub tabulatorów.
- **Zmiany w kodowaniu:** Wykorzystanie podobnie wyglądających znaków Unicode (homoglify).
- **Leksykalne:** Zmiana słów na synonimy, aby zakodować wiadomość w kolejności zmian.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Steganografia Sieciowa (Protokół)

Warstwa Transportowa

Osadzanie informacji w protokołach kontroli sieci, takich jak TCP (np. w polu ID), UDP, czy ICMP.

Nagłówki Pakietów

Wykorzystanie pól w nagłówkach, które są ignorowane przez większość oprogramowania lub mogą zawierać losowe/nieużywane dane (np. pola rezerwowe).

Timing Channels (Kanały Czasowe)

Manipulowanie opóźnieniami między pakietami w celu kodowania wiadomości w czasie transmisji.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Klucze i Zasada Kerckhoffsa

Steganografia Czysta (Pure)

Opiera się na nieznajomości metody przez atakującego (Security by Obscurity). **Nie jest polecana**, ponieważ nie spełnia Zasady Kerckhoffsa. Złamanie metody to złamanie systemu.

Steganografia z Kluczem

Metoda jest jawna. Do osadzenia lub wyodrębnienia wiadomości używany jest **klucz** (prywatny lub publiczny), który muszą znać tylko strony komunikujące się. Jest to bezpieczniejsze podejście.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Legalne Zastosowanie: Cyfrowe Znaki Wodne

Ochrona Praw Autorskich

- Cyfrowe znakowanie wodne (watermarking) to technika steganograficzna wykorzystywana do ukrywania informacji o autorstwie lub właścicielu pliku w samym pliku multimedialnym (obraz, audio, wideo).

- Znak wodny jest niewidzialny lub niemal niewidoczny, ale jest wystarczająco trwały, aby przetrwać kompresję i modyfikacje, umożliwiając identyfikację źródła wycieku lub pirackiej kopii.

Źródło: electronics.howstuffworks.com

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Uwierzytelnianie i Autentyczność Dokumentów

100%

Integralność Danych

Zwalczanie Fałszerstw

Steganografia bywa wykorzystywana przez organy rządowe do zwiększenia bezpieczeństwa dokumentów tożsamości.

Przykładowo, dane biometryczne (np. odcisk palca) mogą być ukryte w zdjęciu na paszporcie w taki sposób, że ludzkie oko nie jest w stanie tego dostrzec, ale maszyna weryfikująca może potwierdzić autentyczność dokumentu w terenie.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

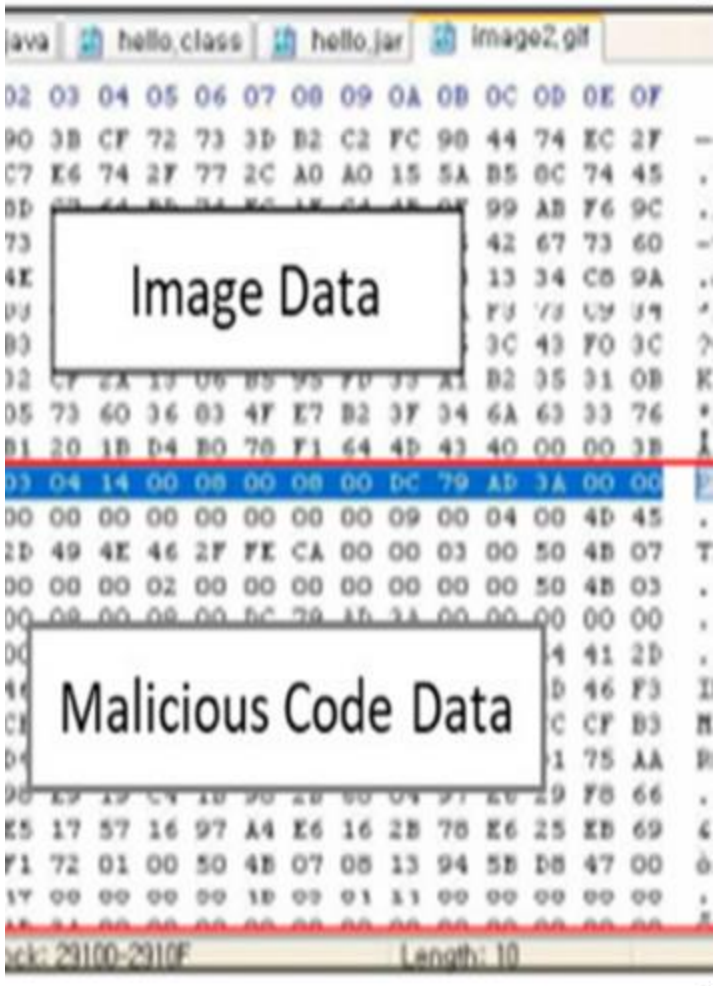
Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Ciemna Strona: Ukrywanie Złośliwego Kodu

Stegano-Malware

Hakerzy i aktorzy zagrożeń wykorzystują steganografię do ukrywania złośliwego oprogramowania (malware) lub poleceń C2 (Command & Control) w pozornie niewinnych plikach, najczęściej obrazach (JPG, PNG).

W ten sposób złośliwy kod omija tradycyjne systemy wykrywania intruzów (IDS), ponieważ plik, który go zawiera, wydaje się być zwykłą grafiką.



Źródło: https://www.mdpi.com

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Steganaliza: Rozpoznanie i Wykrywanie

Nauka zajmująca się atakami na ukrywaną informację. Celem jest wykrycie, czy dany nośnik zawiera ukrytą wiadomość, a następnie jej odzyskanie lub zniszczenie.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Kluczowe Metody Steganalizy

Steganaliza Pasywna

Ogranicza się jedynie do wykrycia, że w danym nośniku **istnieje** ukryta informacja.

Steganaliza Aktywna

Próba **zniszczenia** lub zmodyfikowania ukrytej wiadomości, aby uczynić ją bezużyteczną dla odbiorcy.

Analiza Statystyczna

Wykrywanie subtelnych, nienaturalnych zmian statystycznych w rozkładzie bitów lub pikseli pliku, charakterystycznych dla osadzania danych (np. analiza histogramu).

Porównanie z Oryginałem

Najprostsza, ale nie zawsze możliwa metoda. Polega na porównaniu zmodyfikowanego pliku (stego-plik) z jego czystym, oryginalnym nośnikiem.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Przyszłość: Kierunki Rozwoju

Wzrost Steganalizy

Rozwój zaawansowanych sieci neuronowych zdolnych do wykrywania nawet najmniejszych anomalii w plikach cyfrowych.

Steganografia Kwantowa

Potencjalne wykorzystanie zasad mechaniki kwantowej do tworzenia absolutnie bezpiecznych i niewykrywalnych kanałów komunikacji.

AI i Uczenie Maszynowe

Wykorzystanie sztucznej inteligencji do generowania bardziej złożonych i trudniejszych do wykrycia stego-nośników.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

https://www.bl.uk/images/v5dwkion/production/ebe3174315f5f2000982bf8ffec5e6200ed29ac0-500x341.jpg/a-greek-writing-exercise-from-egypt,-2nd-century-ad-add-ms-34186.jpg?rect=0,40,500,263&w=1200&h=630&auto=format

Źródło: www.bl.uk

https://preview.redd.it/tem6da3izux11.jpg?width=640&crop=smart&auto=webp&s=1084476026da2183131511l6f9889d1a181adaa3

Źródło: www.reddit.com

https://www.mdpi.com/applsci/applsci-14-07119/article_deploy/html/images/applsci-14-07119-g001-550.jpg

Źródło: www.mdpi.com

https://implex.dev/_next/image?url=https%3A%2F%2Fd1by0hsgj87y7x.cloudfront.net%2Finsights%2F2025.01.22-Data%2520Visualization%2520in%2520Website%2520Design%253A%25207%2520Top%2520Examples%2FpictureMobileUrl%2FInsights26-960px.webp&w=3840&q=75

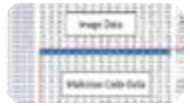
Źródło: implex.dev

https://us1.discourse-cdn.com/cursor1/original/3X/4/2/42f9b7c405dc35fabac82e6b71eea7050e163565.png

Źródło: forum.cursor.com

https://media.hswstatic.com/eyJidWNrZXQiOiJjb250ZW50Lmhzd3N0YXRpYy5jb20iLCJrZXkiOiJnaWZcL3NodXR0ZXJzdG9jay0yMjU5MDc0MDQ5LmpwZyIsImVkaXRzIjp7InJlc2l6ZSI6eyJ3aWR0aCI6ODI4fX19

Źródło: electronics.howstuffworks.com



https://www.mdpi.com/symmetry/symmetry-12-01621/article_deploy/html/images/symmetry-12-01621-g001-550.jpg

Źródło: www.mdpi.com

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Dziękuję za uwagę

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Podstawy kryptografii
Wykład nr 6
Temat: Analiza bezpieczeństwa algorytmów

Dr inż. Marek B.Horyński
Katedra Informatyki Stosowanej

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Plan prezentacji

Plan wykładu

- Wprowadzenie: Problem Zaufania
- Podstawy Kryptograficzne
- Anatomia Podpisu Cyfrowego
- Infrastruktura Klucza Publicznego (PKI)
- Zastosowania i Kontekst Prawny
- Wyzwania i Przyszłość

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Sekcja 1: Kryptografia a Kryptoanaliza

Kryptografia

Dziedzina skoncentrowana na utajnianiu informacji przed tymi, którzy nie mają odpowiednich uprawnień.
Od tysiącleci tworzono i udoskonalano rozwiązania w tym celu. W starożytnej Grecji stosowano np. szyfr wykorzystujący drewniany kij i pas skórzany.

Kryptoanaliza

Koncentruje się na zastosowaniu metod matematycznych i znajomości języków do odszyfrowywania zaszyfrowanych treści. Są dwiema przeciwstawnymi dziedzinami. Pierwsze prace, np. badanie częstości występowania liter, pojawiły się w IX wieku (al-Kindi).

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Modele Ataku – Możliwości Przeciwnika

- **Ciphertext-only (Tylko szyfrogramy):** Atakujący dysponuje wyłącznie zaszyfrowanym tekstem (najsłabszy model).
- **Known-plaintext (Szyfrogram + tekst jawny):** Atakujący zna fragmenty tekstu jawnego i odpowiadające im szyfrogramy.
- **Chosen-plaintext (Szyfrogram + własny tekst):** Atakujący może wybrać dowolny tekst jawny i poznać jego szyfrogram (bardzo silny).
- **Chosen-ciphertext (Wybrany szyfrogram):** Może wybrać szyfrogram do odszyfrowania i uzyskać tekst jawny.
- **Adaptive attacks (Adaptacyjne):** Atakujący dostosowuje swoje działania na podstawie uzyskanych wyników.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Kluczowe Metody Kryptoanalizy Klasycznej i Symetrycznej

Analiza Częstości

Obserwacja powtarzalności znaków (np. Kasiski examination, index of

Atak Brute-Force

Przeszukiwanie całej przestrzeni kluczy.

Kryptoanaliza Różnicowa

Analiza wpływu zmian wejścia na wyniki (kluczowa dla szyfrów blokowych).

Kryptoanaliza Liniowa

Próba znalezienia liniowych zależności między wejściem a wyjściem.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Kryteria Oceny Bezpieczeństwa Algorytmów

Własności Matematyczne

Deterministyczność i brak przewidywalnych wzorców. Odporność na ataki kryptograficzne (np. kryptoanaliza statystyczna).

Kryteria Praktyczne

Rozmiar klucza i efektywność. Łatwość implementacji (ryzyko błędów). Odporność na ataki sprzętowe (side-channel).

Kryteria Formalne (np. NIST)

Formalne dowody odporności dla określonych modeli ataków. Testy odporności w realnych scenariuszach.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Sekcja 2: AES jako Standard Przemysłowy

AES (Advanced Encryption Standard): Symetryczny szyfr blokowy, następca DES. Jest to obecnie najpowszechniej stosowany algorytm symetryczny.

Konstrukcja: Nie bazuje na sieci Feistla. Składa się z transformacji: AddRoundKey, MixColumns, ShiftRows, SubBytes.

Liczba Rund: Zależy od długości klucza (np. 10 rund dla klucza 128-bitowego, 14 dla 256-bitowego).

Zaleta: Przejrzystość zasad opartych na matematyce (w ciele Galois GF(2^8)), co pozwala na formalną analizę.

Opracowanie własne na podstawie norm i przepisów.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

POLLUB z nami nowoczesne technologie

POLITECHNIKA LUBELSKA

Dziękuję za uwagę

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Podstawy kryptografii
Wykład nr 7
Temat: Praktyczne zastosowania kryptografii. Przyszłość kryptografii

Dr inż. Marek B.Horyński
Katedra Informatyki Stosowanej

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

PLAN PREZENTACJI

01 **Szyfrowanie danych**
SSL/TLS, VPN, dyski szyfrowane

02 **Podpisy cyfrowe i PKI**
Certyfikaty, e-podpis, e-commerce

03 **Kryptowaluty i blockchain**
Bitcoin, Ethereum, smart-kontrakty

04 **Obliczenia kwantowe**
Zagrożenia dla RSA i ECC

05 **Kryptografia post-kwantowa**
NIST PQC, algorytmy odporne

06 **Homomorficzne i MPC**
Obliczenia na zaszyfrowanych danych

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

01 / SZYFROWANIE DANYCH W PRAKTYCE

HTTPS / TLS 1.3

Szyfruje cały ruch web – bankowość, e-mail, media społecznościowe.

VPN

Tuneluje dane w sieci publicznej; AES-256 + ECDH w protokołach WireGuard i OpenVPN.

Szyfrowanie dysków

BitLocker (Windows), FileVault (macOS), VeraCrypt; AES-XTS chroni dane w spoczynku.

Szyfrowanie baz danych

Transparent Data Encryption (TDE) w SQL Server, Oracle i PostgreSQL.

95%

stron HTTPS
w Chrome (2024)

AES-256

standard rządowy
USA (NIST FIPS 197)

~1 ms

narzut TLS 1.3
na połączenie

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

02 / PODPISY CYFROWE I PKI

Kwalifikowany e-podpis

Równoważny prawnie podpisowi odręcznemu w UE (eIDAS).

Certyfikaty SSL/TLS

CA podpisuje certyfikat serwera; przeglądarka weryfikuje łańcuch.

Podpisywanie kodu

Microsoft, Apple i Google wymagają podpisanych paczek (codesign).

Bankowość i e-commerce

3D Secure, BLIK, PSD2 – silne uwierzytelnianie klientów.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

03 / KRYPTOWALUTY I BLOCKCHAIN

Kryptografia asymetryczna (secp256k1)
Para kluczy ECDSA: klucz prywatny = własność środków;
klucz publiczny = adres portfela.

~21M
limit BTC
(entropia klucza pryw.)

Funkcje skrótu (SHA-256)

Każdy blok zawiera hash poprzedniego – niezmienialność łańcucha. Mining = znajdowanie nonce z Proof-of-Work.

2^{160}

przestrzeń adresów Ethereum

Smart-kontrakty (Ethereum)
Bytecode na EVM; logika biznesowa bez pośredników.
Zero-knowledge proofs w rollupach L2.

ZKP
Zcash, Aztec, StarkNet

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

04 / OBLICZENIA KWANTOWE – ZAGROŻENIA

Algorytm	Rozmiar klucza dziś	Bezpieczeństwo kwantowe	Atak kwantowy
RSA-2048	2048 bit	Zagrożony	Algorytm Shora
ECC-256	256 bit	Zagrożony	Algorytm Shora
AES-128	128 bit	Osłabiony	Algorytm Grovera (→ 64-bit)
AES-256	256 bit	Akceptowalny	Algorytm Grovera (→ 128-bit)
SHA-256	256 bit	Akceptowalny	Grover – minimalny wpływ

CRYPTOGRAPHICALLY RELEVANT QUANTUM COMPUTER (CRQC): szacowany ok. 2030–2035

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

05 / KRYPTOGRAFIA POST-KWANTOWA (PQC)

NIST PQC 2024 – Standardy zatwierdzone

CRYSTALS-Kyber (ML-KEM)	CRYSTALS-Dilithium (ML-DSA)
Rodzina: Kratki	Rodzina: Kratki
Zastosowanie: Wymiana kluczy (KEM)	Zastosowanie: Podpisy cyfrowe

FALCON (FN-DSA)	SPHINCS+ (SLH-DSA)
Rodzina: NTRU / Kratki	Rodzina: Drzewa skrótów
Zastosowanie: Podpisy (małe kl.)	Zastosowanie: Podpisy (bez kratki)

Google, Apple i Cloudflare już wdrażają ML-KEM w TLS 1.3 (hybridowe tryby X25519+Kyber768)

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

06 / HOMOMORFICZNE SZYFROWANIE I MPC

Fully Homomorphic Encryption (FHE)

- Obliczenia na zaszyfrowanych danych bez odszyfrowania.
- Pionierzy: Craig Gentry (2009) – pierw. pełny schemat.
- Schematy: BFV, CKKS, TFHE – biblioteki: SEAL, OpenFHE, HElib.
- Zastosowania: ML na prywatnych danych (Google, Microsoft Azure), medycyna, finanse.
- Wyzwanie: ~1000× wolniejsze niż operacje na jawnych danych (aktywne badania nad akceleracją FPGA/ASIC).

Multi-Party Computation (MPC)

- Strony wspólnie obliczają funkcję bez ujawniania wejść.
- Protokoły: Garbled Circuits, Secret Sharing (Shamir), SPDZ.
- Zastosowania: przetargi, portfele kryptowalut bez HSM, aukcje.
- Threshold Signatures (TSS): zastępuje multisig; używany przez Fireblocks, ZenGo.
- MPC + ZKP = podstawa prywatnych rolupów (Aztec, Aleo).

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

MAPA DROGOWA PRZYSZŁOŚCI KRYPTOGRAFII

2024–2025	2026–2028	2028–2030	2030–2035
NIST PQC standard	Migracja TLS do PQC hybryd	FHE akceleracja hardwarowa	CRQC – migr. krytyczna

Kwantowe klucze (QKD)

Dystrybucja kluczy kanałem kwantowym – nieodwracalność fizyczna.

Kryptografia oparta na ID

Klucz prywatny = tożsamość (biometria, DID).

ZK-SNARKs / STARKs

Dowody zerowej wiedzy bez zaufanej konfiguracji.

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

POLLUB z nami nowoczesne technologie

POLITECHNIKA LUBELSKA

PODSUMOWANIE

Kryptografia: fundament cyfrowego świata

- Szyfrowanie chroni miliardów użytkowników każdego dnia.
- Podpisy cyfrowe zapewniają autentyczność i niewyparcie.
- Blockchain i ZKP tworzą nową warstwę zaufania.
- Era kwantowa wymaga natychmiastowej migracji do PQC.
- FHE i MPC otwierają erę obliczeń na prywatnych danych.

"Cryptography is the ultimate form of non-violent direct action." – Julian Assange

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Dziękuję za uwagę

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską