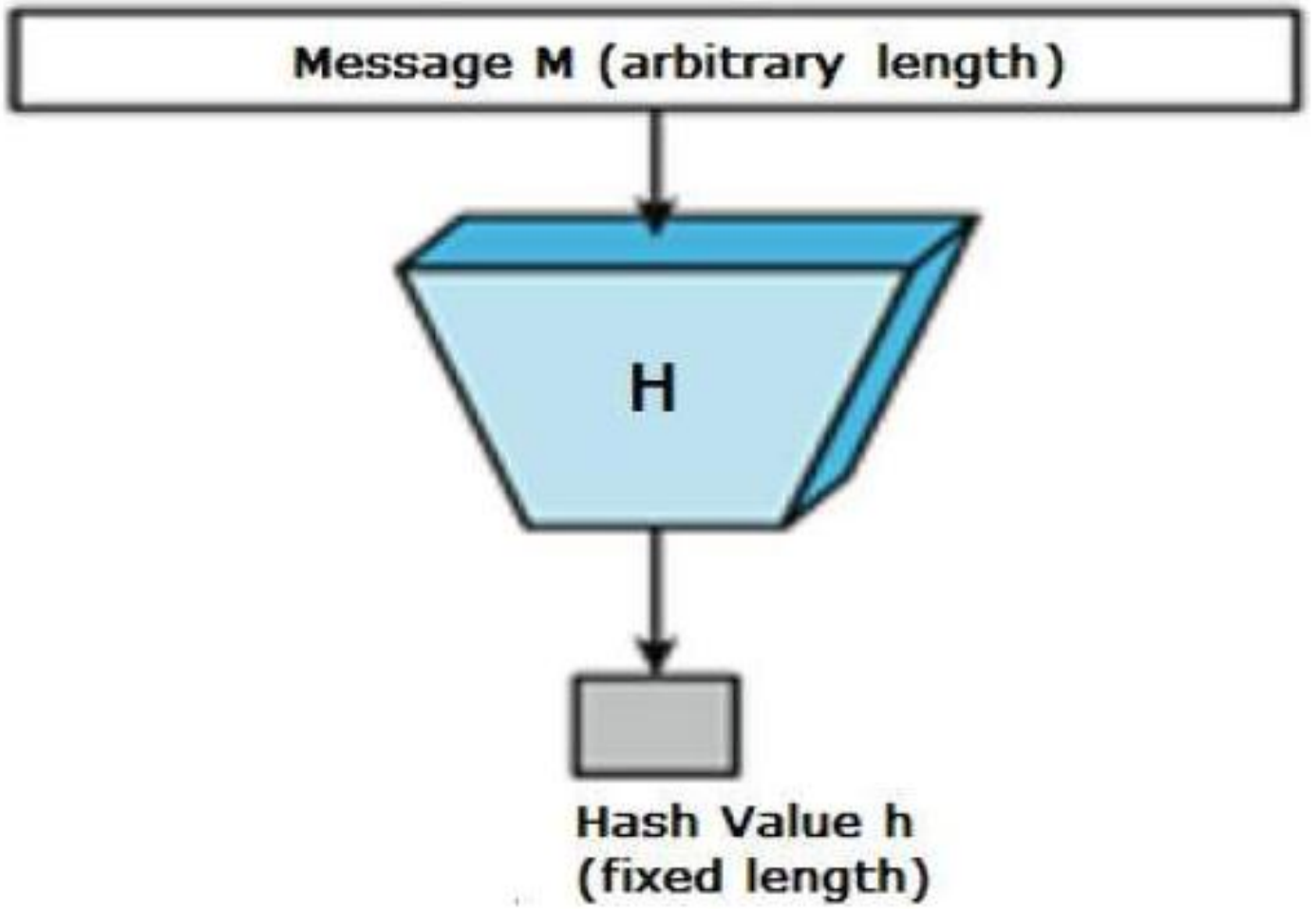
BEZPIECZEŃSTWO W KRYPTOGRAFII

PIOTR DOBOSZ

FUNKCJE SKRÓTU

- Znane powszechnie jako funkcje mieszające lub hash functions
- Zadaniem funkcji jest matematyczne przekształcenie wejścia numerycznego w skompresowaną wartość numeryczną (inną od wejściowej)
- Wejście może mieć dowolną długość (ustaloną), zaś wyjście ma zawsze taką samą długość
- Wynik nazwywa się często strzeszczeniem (digest message) bądź tzw. hashem

FUNKCJE SKRÓTU



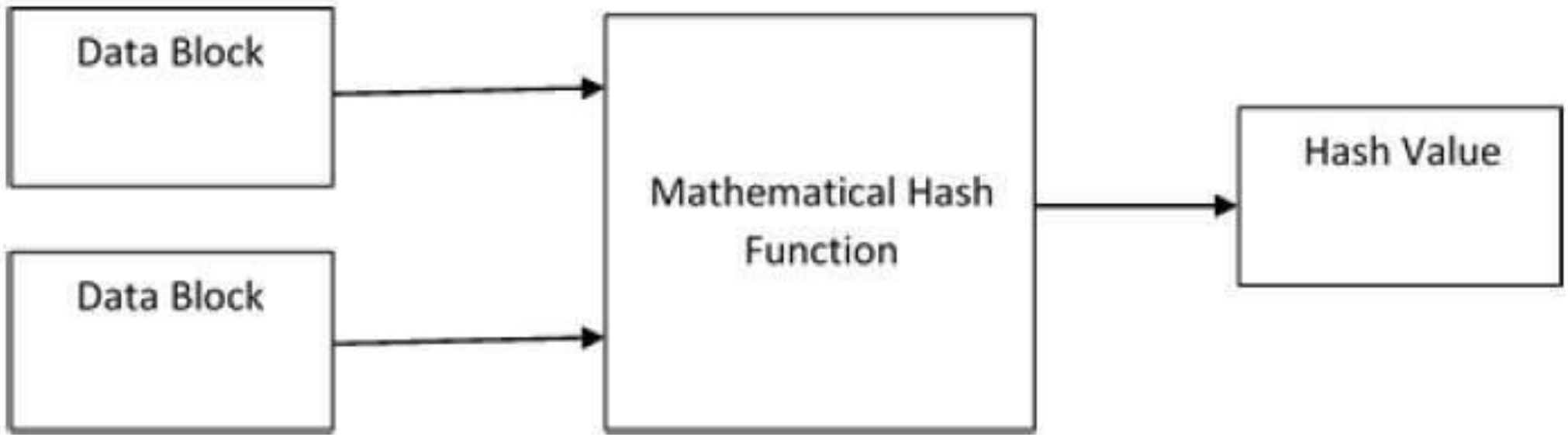
FUNKCJE SKRÓTU

- Ponieważ wyjście jest stałe i przeważnie mniejsze od wejścia, niekiedy funkcje te nazwya się funkcjami kompresji
- Ilość bitów wyjścia odpowiada ilości bitów w funkcji; często stosowane funkcje to 160-512 bitowe (chociaż mogą być mniejsze/większe)
- Funkcje skrótu to szybkie operacje, znacznie szybsze niż szyfrowanie symetryczne

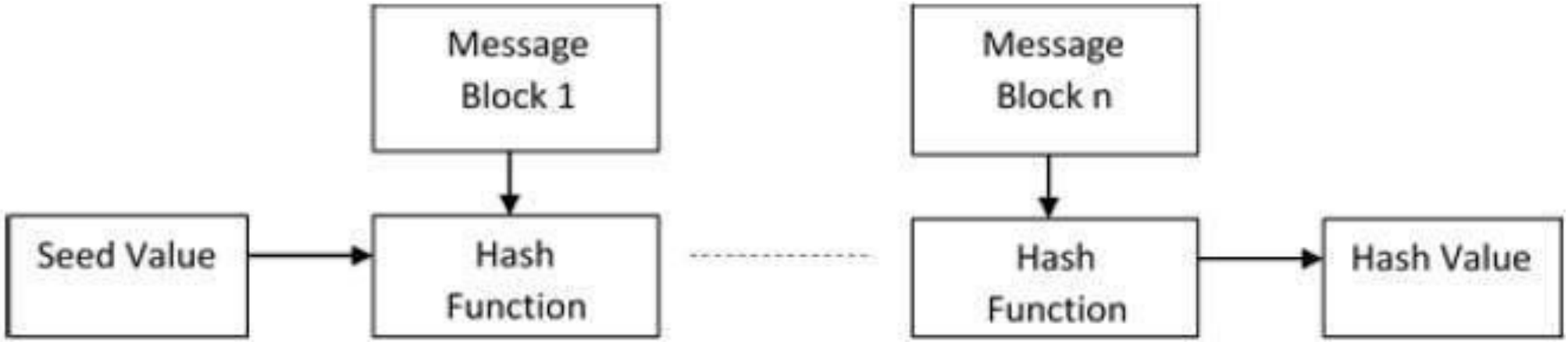
WŁAŚCIWOŚCI FUNKCJI SKRÓTU

- Odporne na znalezienie źródła z wygenerowanego skrótu
- Odporne na odnalezienie źródła poprzez podobieństwo wyników funkcji
- Odporne na znalezienie dwóch wejść dających identyczny skrót

DZIAŁANIE FUNKCJI SKRÓTU



DZIAŁANIE FUNKCJI SKRÓTU



MESSAGE DIGEST (MD)

- 128-bitowa funkcja zatwierdzona jako standard internetowy RFC 1321
- Należy do rodziny algorytów MD2, MD4, MD6
- Używany do sprawdzania sum kontrolnych plików
- W 2004 wykryto w nim podatność na kolizję

SECURE HASH FUNCTION/ALGORITHM (SHA)

- SHA-0 został opublikowany przez NIST (National Institute of Standards and Technology) w 1993 roku; 160 bitowy
- Po opublikowaniu podatności w 1995 roku niezalecany do użytku;
- Wdrożono nową wersję protokołu, SHA-1; przez dłuższy czas najbezpieczeniejszy standard, aż do 2005 (odkryto lukę z kolizjami)
- Wprowadzono SHA-2, z wariantem 224,256,384,512; nie odnotowano ataku na tę wersję algorytmu
- W 2012 pokazano standard SHA-3 z dodatkowymi poprawkami bezpieczeństwa

RACE INTEGRITY PRIMITIVES EVALUATION MESSAGE DIGEST (RIPEMD)

- Opracowany przez otwartą grupę (społeczność); znany także jako Europejskie standardy funkcji skrótu
- Wersja 128-bitowa bazowała na rozwiązaniach MD-4 (stąd uznana za niebezpieczną)
- Wersje 160 i 320; nie ma dowodów na ich łamanie czy złamanie; wersje te nie różnią się pod kątem bezpieczeństwa RIPEMD-128/RIPEMD-160

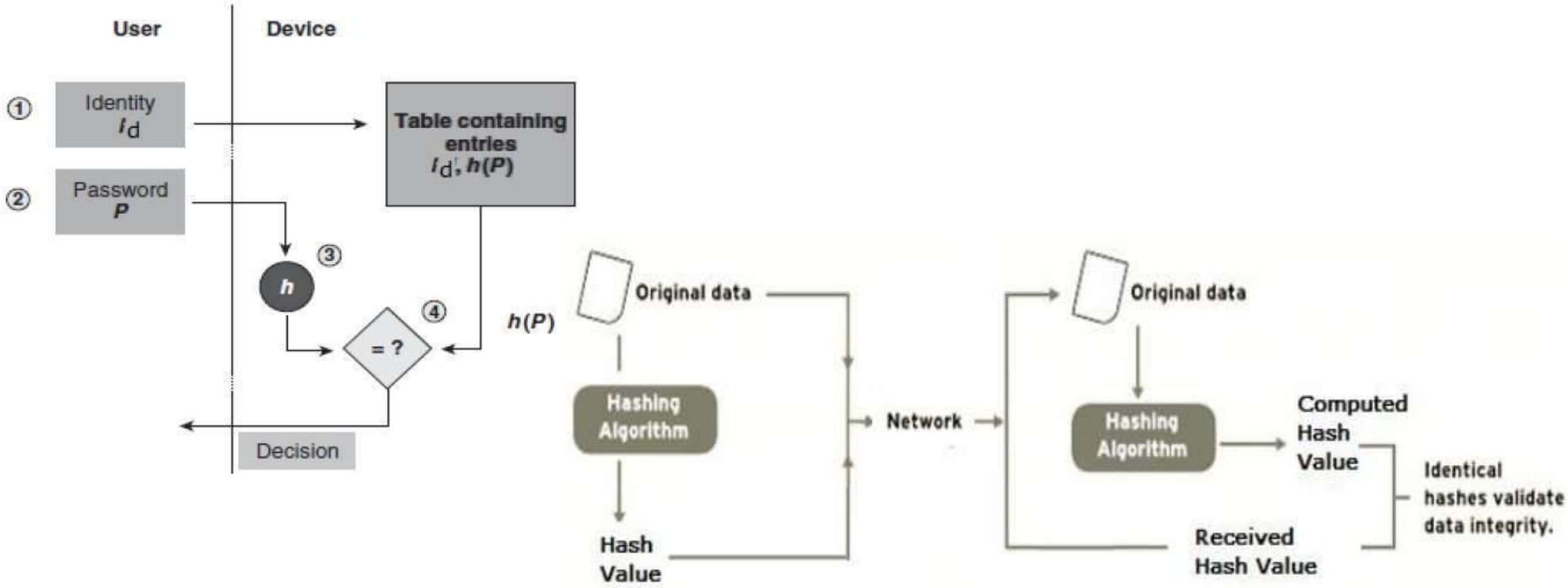
WHIRLPOOL

- 512 bitowa funkcja haszująca; pochodna AES (projektował tę funkcję Vincent Rijmen, współtwórca AES)
- Obecnie funkcjonują 3 wersje standardu: WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.

ZASTOSOWANIE FUNKCJI SKRÓTU

- Przechowywanie hasła
- Sprawdzanie integralności danych

ZASTOSOWANIE FUNKCJI SKRÓTU



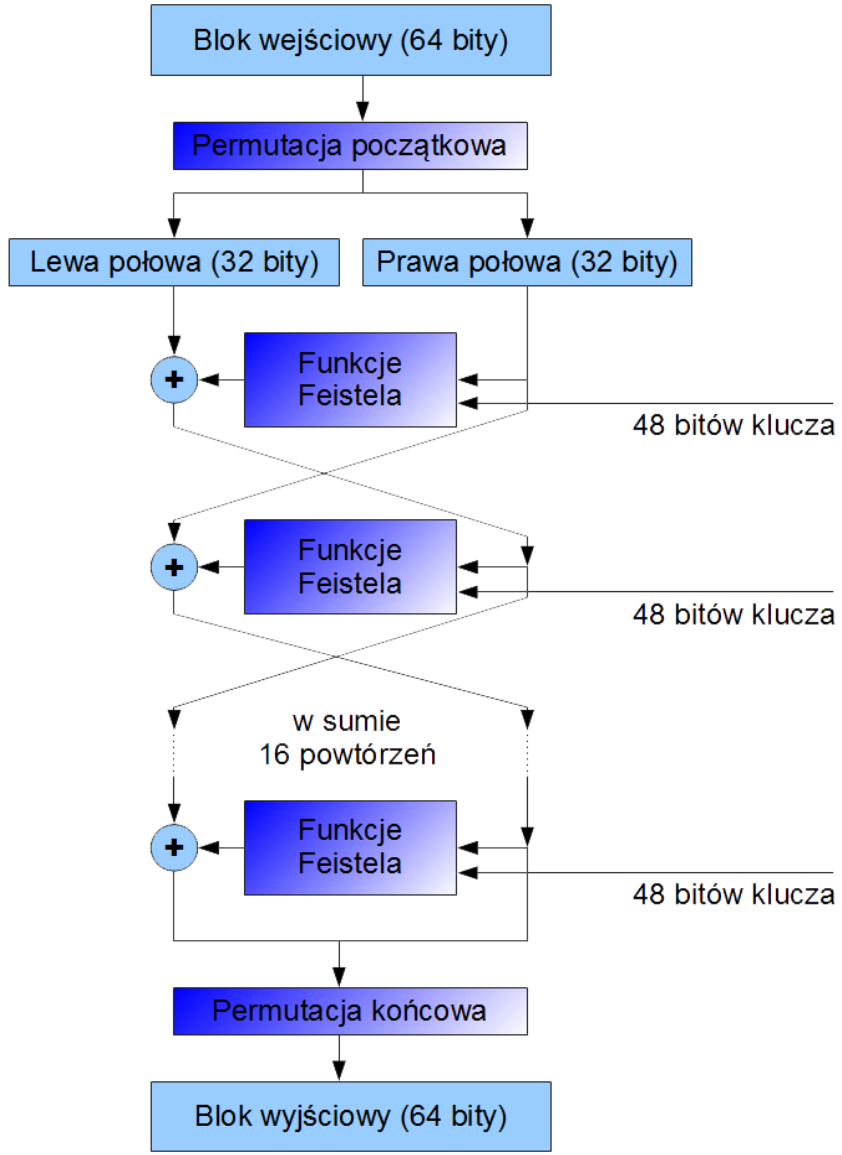
KRYPTOGRAFIA SYMETRYCZNA

- Stosuje jeden klucz do szyfrowania i deszyfrowania
- Szybsza niż kryptografia asymetryczna
- Niestety bardziej podatna na podsłuch
- Szerokie zastosowanie w codziennym użytku

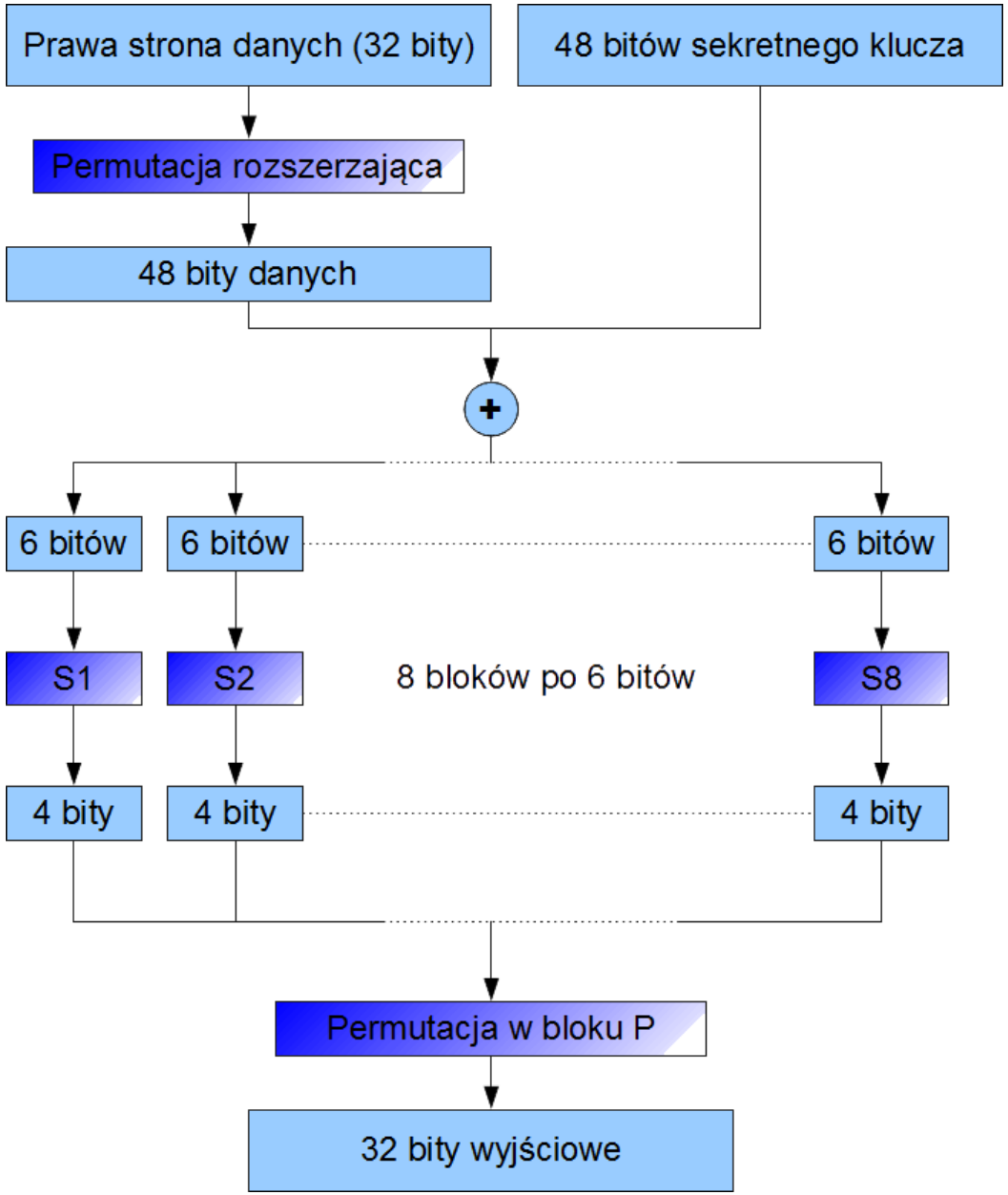
DATA ENCRYPTION STANDARD (DES)

- Inna nazwa to DEA (Data Encryption Algorithm)
- Opracowany przez IBM w latach 70 XX wieku, wprowadzony jako standard szyfrowania w 1977 (USA)
- Pierwotnie 58 bitowy (+8 bitów parzystości)
- Modyfikacja, Triple-DES (TDES, TDEA, 3DES) używa 3 kluczy (paczka 3 podstawowych kluczy DES); 168 bit
- Istnieje wariant z dwoma kluczami (2DES, 2TDEA); 112 bitowy, jednak nie zwiększa ani efektywności ani bezpieczeństwa
- Podatny na atak "Sweet 32"

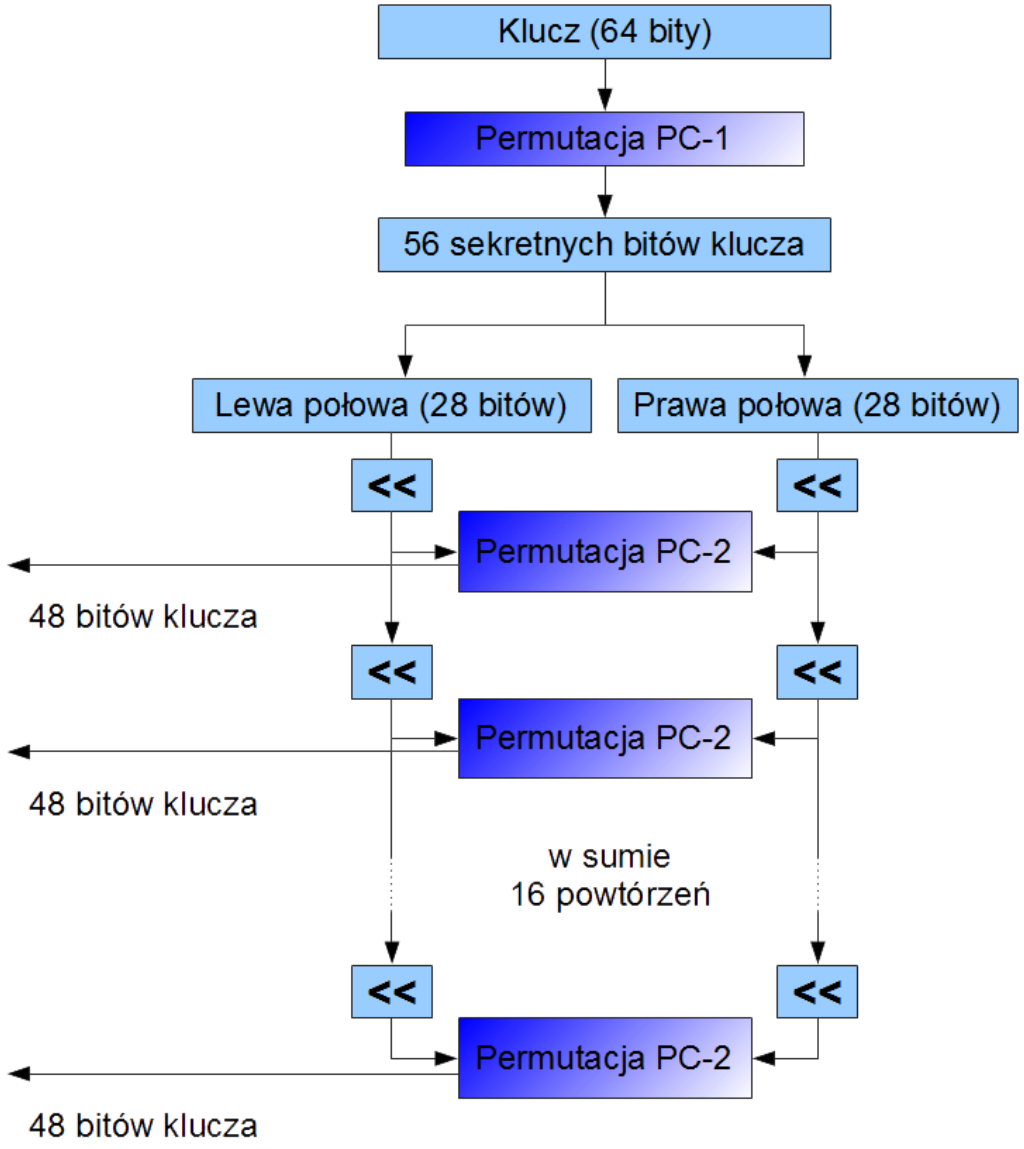
DES


Blok wejściowy (64 bity)
Permutacja początkowa
Lewa połowa (32 bity)
Prawa połowa (32 bity)
Funkcje Feistela
48 bitów klucza
Funkcje Feistela
48 bitów klucza
w sumie 16 powtórzeń
Funkcje Feistela
48 bitów klucza
Permutacja końcowa
Blok wyjściowy (64 bity)

DES –FEIST FUNCTION



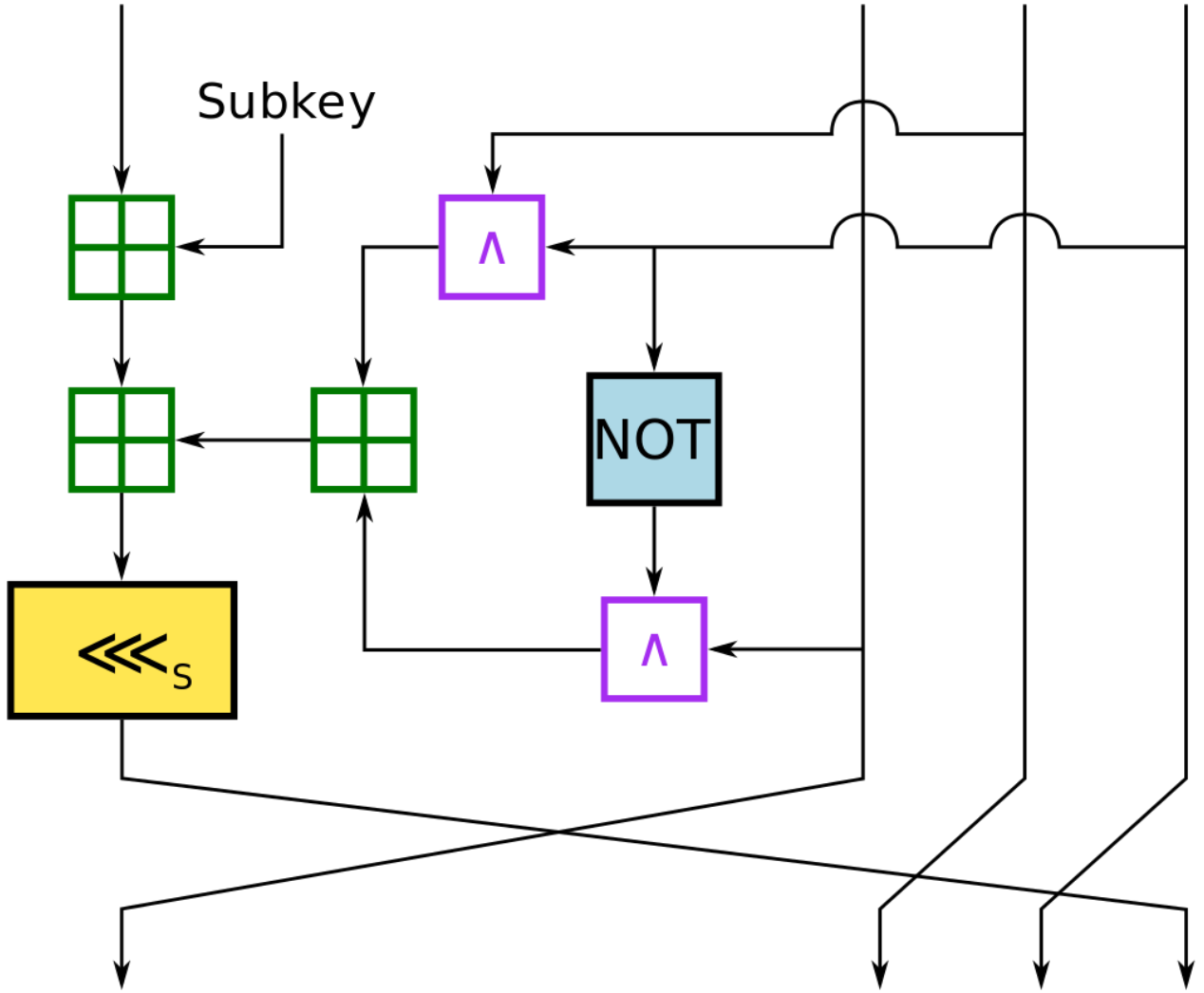
DES – BIT GENERATION



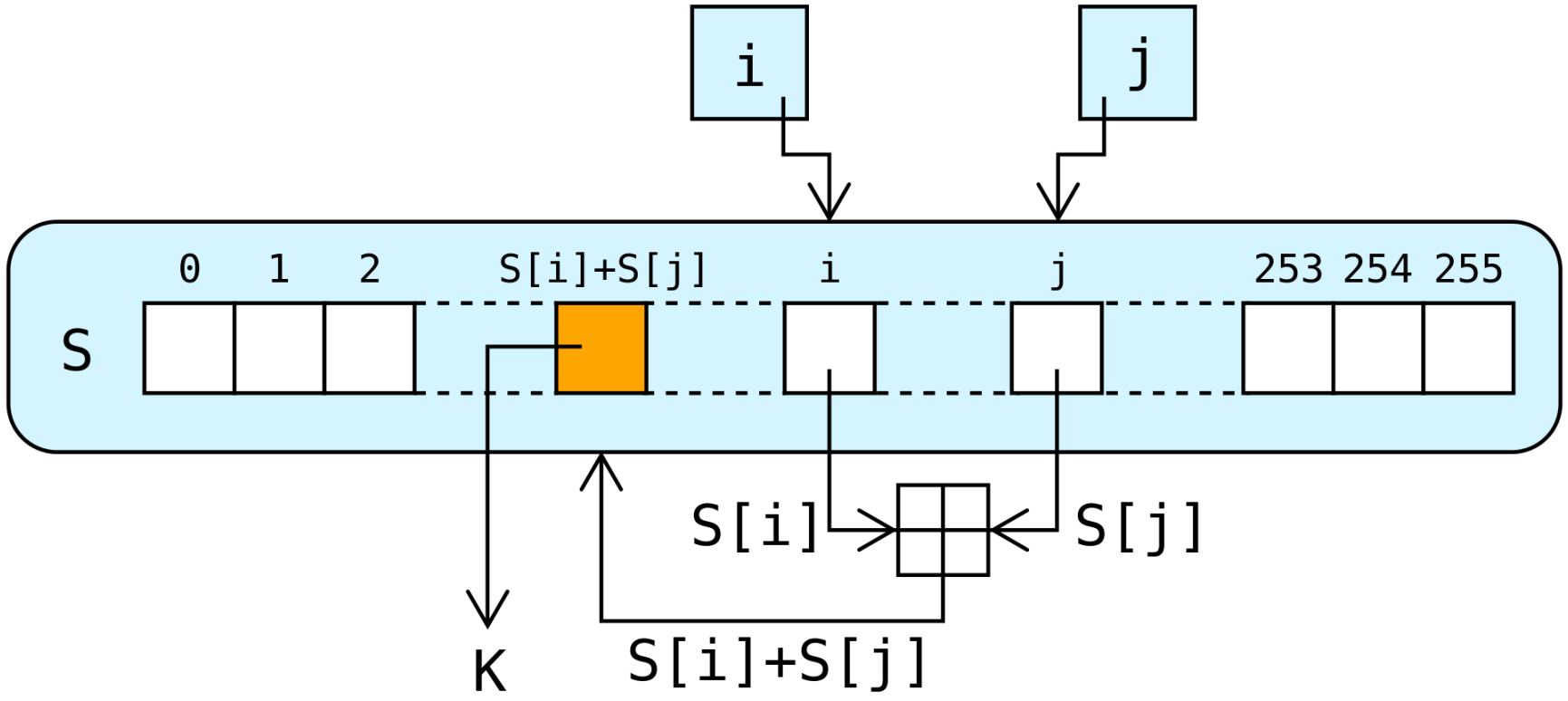
RON'S CODE/RIVEST'S CIPHER (RC)

- Zestaw algorytmów symetrycznych stworzony przez Rona Rivesta
- RC1 oraz RC3 nigdy nie zostały użyte (RC1 nie został opublikowany, RC3 został złamany przed upublicznieniem)
- RC2 jest 64bitowy (z możliwością używania 128 bitów)
- RC4 to tzw. Szyfrowanie strumieniowe, wykorzystywane w SSL/TLS oraz WLAN
- RC5 wprowadza bloki 32/64/128 bit oraz zmienną długość klucza (do 2048 bit), zaś ilość przebiegów może wynosić nawet 255
- RC6 posiada stały blok 128 bit, zgłoszony do konkursu zabezpieczeń WPA

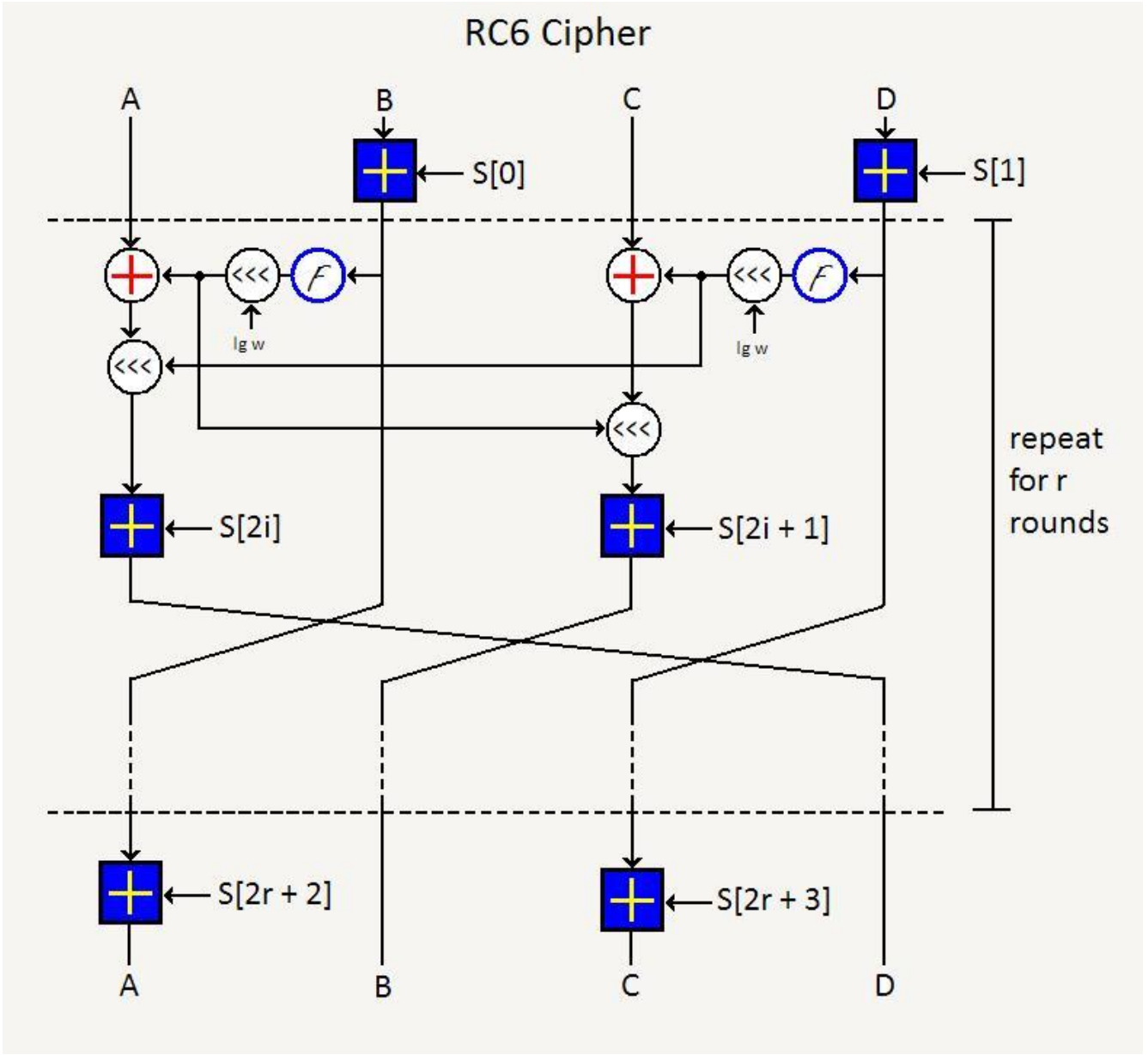
RC2



RC4



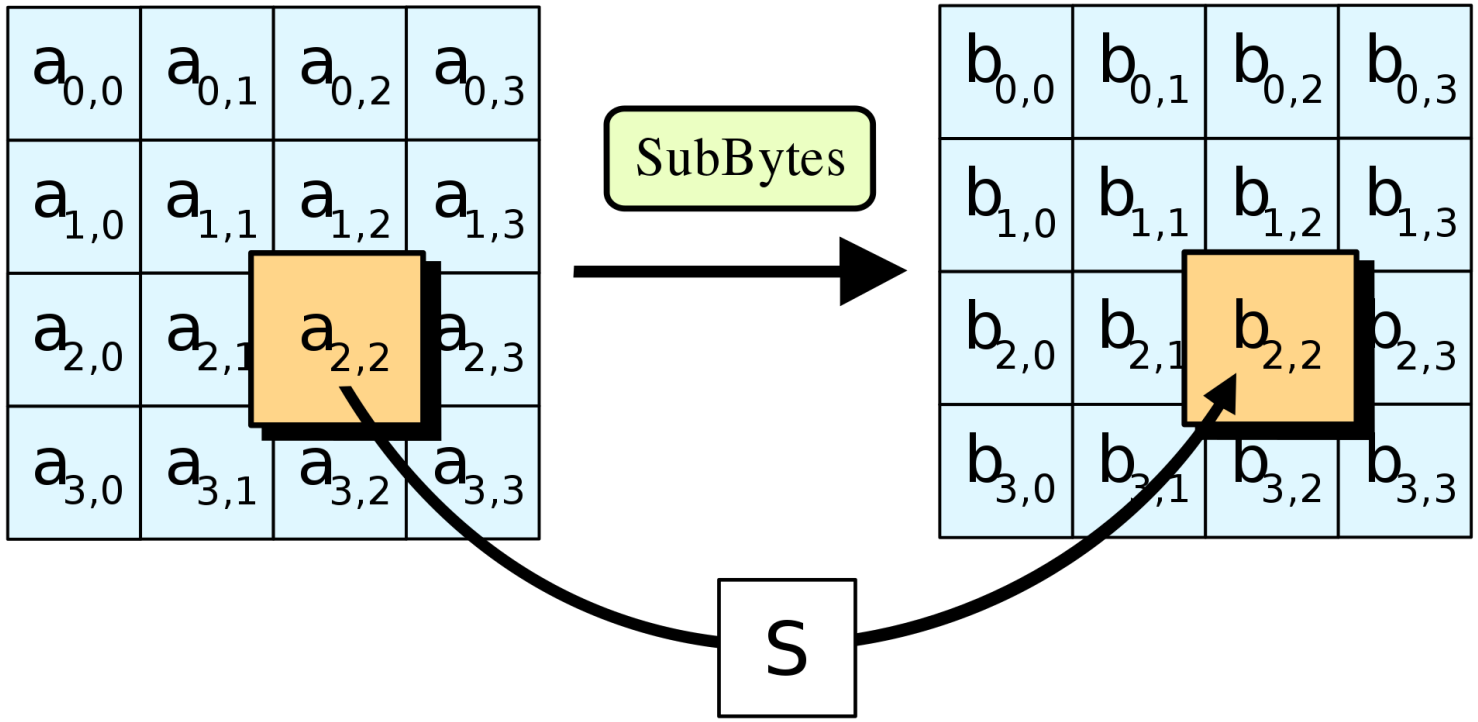
RC6


RC6 Cipher
A
B
C
D
S[0]
S[1]
<<<
f
lg w
S[2i]
S[2i + 1]
repeat
for r
rounds
S[2r + 2]
S[2r + 3]
A
B
C
D

ADVANCED ENCRYPTION STANDARD (AES)/RIJNDAEL

- Stworzony przez Joana Daemena i Vincenta Rijmena
- Posiada stałą wielkość bloku 128 bit, zmienne długości klucza – 128, 192 oraz 256 bit
- Jedyny z rekomendacją TOP SECRET służ US (wojsko i ochrona)

AES


a0,0 a0,1 a0,2 a0,3
a1,0 a1,1 a1,2 a1,3
a2,0 a2,1 a2,2 a2,3
a3,0 a3,1 a3,2 a3,3
SubBytes
b0,0 b0,1 b0,2 b0,3
b1,0 b1,1 b1,2 b1,3
b2,0 b2,1 b2,2 b2,3
b3,0 b3,1 b3,2 b3,3
S

AES

Rozmiar klucza używany w algorytmie określa liczbę powtórzeń transformacji, które przekształcają dane wejściowe (czyli tekst jawny) w dane wyjściowe (szyfrogram). Liczba cykli powtórzeń jest następująca:

- 10 cykli powtórzeń dla klucza 128-bitowego;
- 12 cykli powtórzeń dla klucza 192-bitowego;
- 14 cykli powtórzeń dla klucza 256-bitowego.

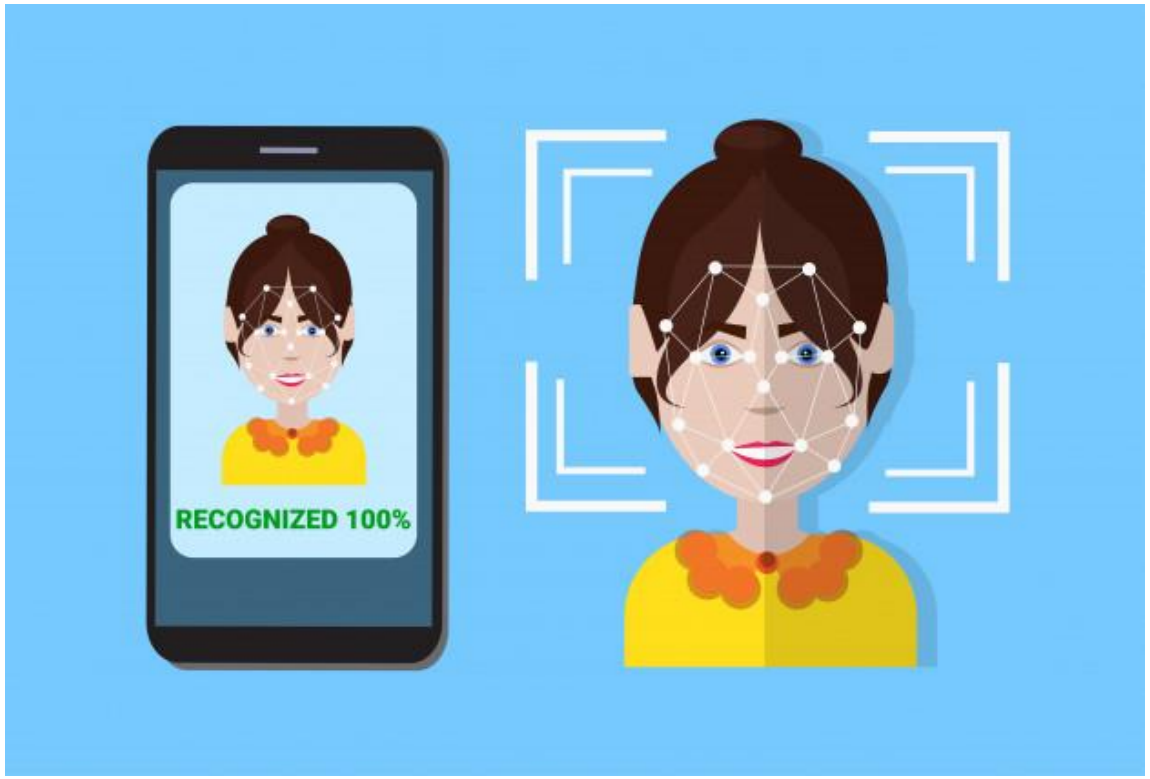
AES

- Rozszerzenie klucza – z głównego klucza algorytmu "tworzy się" kolejne klucze. AES wymaga osobnego klucza 128-bitowego dla każdej rundy, plus jeden dodatkowy.
- runda wstępna
  - Dodawanie klucza rundy – każdy bajt macierzy stanu jest mieszany z blokiem rundy za pomocą operatora bitowego XOR.
- Rundy
  - Zamiana Bajtów – nieliniowa zamiana, podczas której każdy bajt jest zamieniany innym.
  - Zamiana Wierszy – etap transpozycji, podczas którego trzy ostatnie wiersze macierzy stanu są cyklicznie zmieniane określoną ilość razy.
  - Mieszanie Kolumn – Operacja odnosi się do kolumn macierzy. Polega na łączeniu czterech bajtów w każdej kolumnie.
  - Dodaj klucz rundy
- Final Round (brak operacji Mieszania Kolumn)
  - Zamiana Bajtów
  - Zamiana Wierszy
  - Dodaj klucz rundy.

KRYPTOGRAFIA SPRZĘTOWA

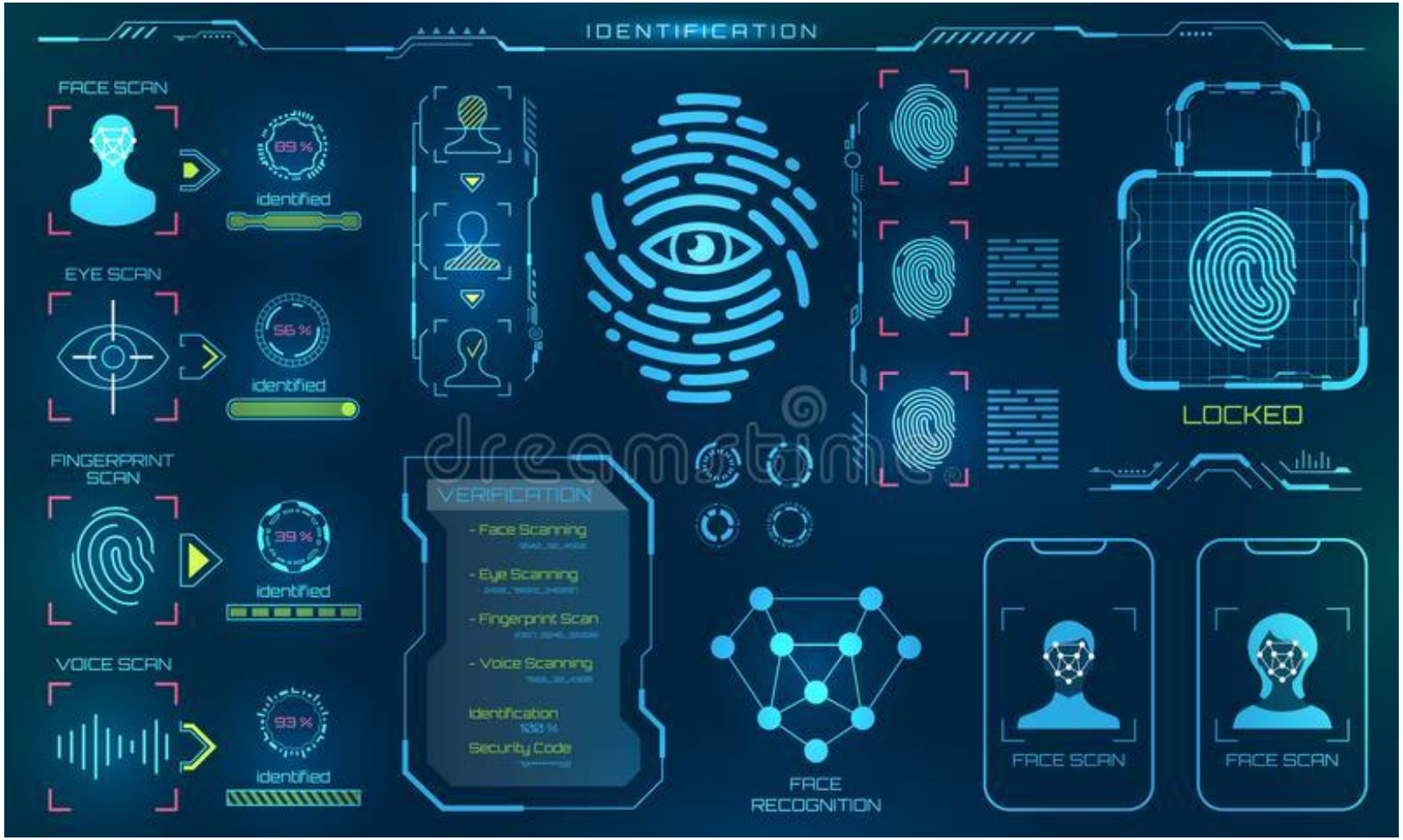
- TPM – Trusted Platform Module
- Podpis cyfrowy
- Biometria

BIOMETRIA



https://image.freepik.com/free-vector/biometric-scanning-system-of-control-protection-smart-phone-scan-user-face-facial-recognition-technology-concept_48369-14860.jpg

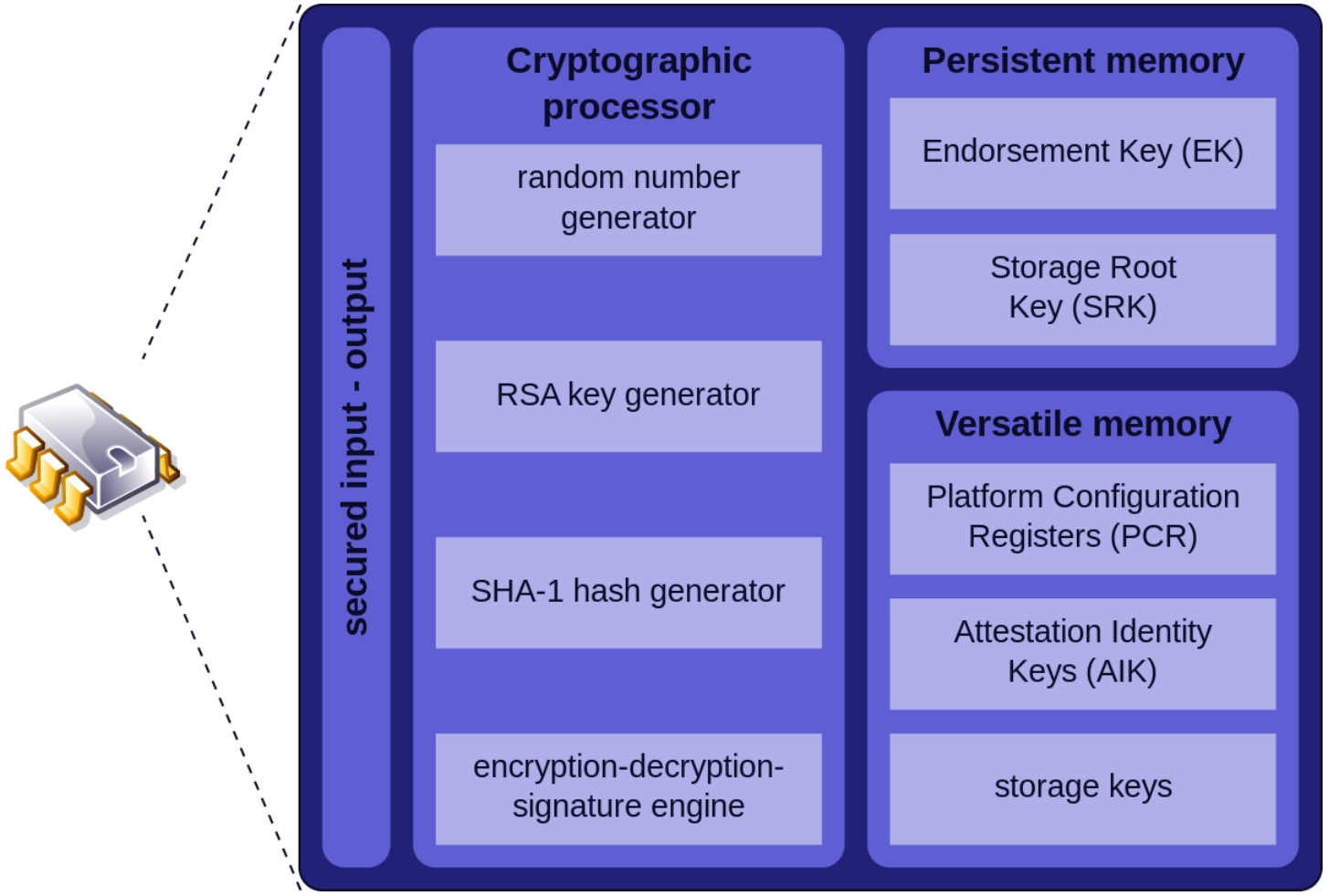
BIOMETRIA



https://thumbs.dreamstime.com/b/biometric-identification-recognition-system-person-line-icons-identity-verification-sign-biometric-identification-116370985.jpg

TPM

https://upload.wikimedia.org/wikipedia/commons/thumb/b/be/TPM.svg/1200px-TPM.svg.png



PODPIS CYFROWY

https://hrm-soft.com/img/software-2018/how-to-apply-digital-signature-2.jpg

ATAKI KRYPTOANALITYCZNE

- ataki możliwe do przeprowadzenia bez znajomości jakichkolwiek informacji, poza pojedynczym szyfrogramem (tekstem tajnym);
- ataki możliwe do przeprowadzenia przy znajomości wielu szyfrogramów;
- ataki możliwe do przeprowadzenia przy znajomości algorytmu i szyfrogramu (-ów) (zobacz: Atak z szyfrogramem);
- ataki możliwe do przeprowadzenia przy znajomości tekstu jawnego i szyfrogramu (zobacz: atak ze znanym tekstem jawnym);
- ataki możliwe do przeprowadzenia przy możliwości wybrania tekstu jawnego (np. możemy spowodować, że ktoś zaszyfruje podstawioną przez nas wiadomość);

ATAKI KRYPTOANALITYCZNE

- zwykle użytkownik wybiera klucz szyfrujący. 90% ludzi używa w tym celu łatwych do zgadnięcia fraz lub słów. Bezpieczeństwo faktyczne kryptosystemu zależy zarówno od algorytmu, jak i od rozmiaru przestrzeni faktycznie używanych kluczy (atak słownikowy);
- wybranie zbyt skomplikowanego klucza zwykle pociąga za sobą konieczność jego zapisania (ataki socjotechniczne)
- szyfrowanie zwykle jest przeprowadzane przez oprogramowanie komercyjne, często pisane bez właściwej analizy implementacji skądinąd doskonałych algorytmów szyfrowania. Nawet najbezpieczniejszy algorytm szyfrowania nie zapewnia bezpieczeństwa, jeśli został niewłaściwie zaimplementowany (np. użyto zbyt prymitywnego generatora liczb losowych);
- oprogramowanie działa w środowisku systemu operacyjnego, który zwykle (dla typowych, popularnych systemów operacyjnych) nie posiada mechanizmów zabezpieczających przed np. odczytaniem danych z pamięci czy z klawiatury w momencie ich zapisywania, lub np. odtworzenia możliwych ziaren generatora liczb losowych (jeśli np. używa się jako ziarna danych z zegara systemowego);
- oprogramowanie działa w środowisku z dostępem do sieci Internet, co ułatwia zastosowanie modyfikowanych ataków słownikowych;

ATAKI NA ALGORYTMY SZYFROWANIA

- atak w oparciu o słabość algorytmu
- atak brute force;
- ataki statystyczne
- meet in the middle
- atak przez analizę różnicową;
- atak urodzinowy;
- atak algebraiczny;

MATERIAŁY I ŹRÓDŁA

- https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
- https://www.geeksforgeeks.org/what-are-hash-functions-and-how-to-choose-a-good-hash-function/
- https://www.sciencedirect.com/topics/computer-science/symmetric-key-algorithm
- https://en.wikipedia.org/wiki/Data_Encryption_Standard
- http://www.crypto-it.net/pl/symetryczne/des.html
- https://en.wikipedia.org/wiki/RC_algorithm
- https://pl.wikipedia.org/wiki/Advanced_Encryption_Standard
- https://www.vida.pl/czym-jest-trusted-platform-module-i-jaka-funkcje-spelnia-w-szyfrowaniu/
- https://sweet32.info/
- https://pl.wikipedia.org/wiki/Atak_kryptologiczny
- https://pl.wikipedia.org/