



**KAPITAŁ LUDZKI**  
NARODOWA STRATEGIA SPÓJNOŚCI

**UNIA EUROPEJSKA**  
EUROPEJSKI  
FUNDUSZ SPOŁECZNY



Piotr Wasilewski

# Bezpieczeństwo danych

---

Zadanie nr 14 – Studia podyplomowe „Bezprzewodowe systemy nadzoru i monitorowania”

Prezentacja multimedialna  
współfinansowana przez Unię Europejską  
w ramach Europejskiego Funduszu Społecznego  
w projekcie

*„Innowacyjna dydaktyka bez ograniczeń  
– zintegrowany rozwój Politechniki Łódzkiej –  
zarządzanie Uczelnią,  
nowoczesna oferta edukacyjna  
i wzmacniania zdolności do zatrudniania  
osób niepełnosprawnych”*



**Politechnika Łódzka**  
Instytut Elektroniki

90-924 Łódź, ul. Żeromskiego 116,  
tel. 042 631 28 83  
[www.kapitalludzki.p.lodz.pl](http://www.kapitalludzki.p.lodz.pl)



# Plan prezentacji

- ❖ Pojęcie bezpieczeństwa
- ❖ Identyfikacja i uwierzytelnianie
- ❖ Szyfrowanie
- ❖ Potwierdzanie autentyczności





# Pojęcie bezpieczeństwa

- Rodzaje bezpieczeństw
- Atrybuty bezpieczeństwa
- Elementy bezpieczeństwa



# Bezpieczeństwo

- bezpieczeństwo publiczne
- bezpieczeństwo bierne
- bezpieczeństwo czynne
- bezpieczeństwo i higiena pracy
- bezpieczeństwo ruchu drogowego
- bezpieczeństwo socjalne
- bezpieczeństwo energetyczne
- **bezpieczeństwo teleinformatyczne**



# Bezpieczeństwo teleinformatyczne

- Niczym niezakłócone funkcjonowanie systemu teleinformatycznego w czasie realizacji przez niego standardowych zadań świadczonych dla dobra instytucji.



# Bezpieczeństwo teleinformatyczne

- Aspekt techniczny
  - integralność
  - poufność
  - dostępność
  - autentyczność
  - rozliczalność
  - niezawodność



# Bezpieczeństwo teleinformatyczne

- System obsługuje człowiek – problemy pozatechniczne – prawo, socjologia, psychologia, kultura.
- Aspekt ekonomiczny:
  - nakłady bezpośrednie
  - nakłady pośrednie
  - dodatkowy nakład pracy



# Trudności

- Systemy teleinformatyczne są złożone, rozproszone, zróżnicowane i szybkie.
- Systemy teleinformatyczne i ich otoczenie wciąż się zmieniają.
- Zagrożenia podlegają ciągłym zmianom i są trudne do pełnego rozpoznania.
- Wiele zagadnień jest trudnych do identyfikacji i nieprzewidywalnych.





# Atrybuty bezpieczeństwa

- **Polska Norma PN-13335-1:**
- **Poufność (confidentiality)** – gwarantuje, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.
- **Autentyczność (authenticity)** – zapewnia, że tożsamość podmiotu lub zasobu jest zgodna z deklarowanym. Dotyczy użytkowników, procesów, systemów, całych instytucji.



# Atrybuty bezpieczeństwa

- Dostępność (availability) – bycie dostępnym i możliwym do wykorzystania na żądanie w założonym czasie (zgodnie z przysługującymi prawami).
- Integralność danych (data integrity) – dane nie zostały zmienione, zniszczone w sposób nieautoryzowany



# Atrybuty bezpieczeństwa

- Integralność systemu (system integrity) – system realizuje zamierzone funkcje w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej
- Integralność (integrity) – integralność danych oraz systemu



# Atrybuty bezpieczeństwa

- Rozliczalność (accountability) – działanie podmiotu (np. użytkownika) może być w jednoznaczny sposób przypisane tylko temu podmiotowi.
- Niezawodność (reliability) – spójne, zamierzone zachowanie i skutki.



# Elementy bezpieczeństwa

- Wrażliwość informacji (sensiblity) – pewna miara ważności przypisana informacji przez jej autora lub dysponenta w celu wskazania konieczności jej ochrony.

Informacja ma charakter abstrakcyjny.

Dane wyrażają informację za pomocą kodu i związane są z nośnikiem.





# Elementy bezpieczeństwa

- Usługa krytyczna (critical service) – usługa realizowana przez STI, mająca bezpośrednie znaczenie dla funkcjonowania instytucji i wskazana przez upoważnione osoby do otoczenia jej szczególną ochroną (szczególnie w zakresie dostępności).
- Zasoby, aktywa (assets) – wszystko co dla instytucji ma wartość i co powinno być chronione.



# Elementy bezpieczeństwa

- Zagrożenie (threat) – potencjalna przyczyna niepożądanego incydentu, który może spowodować szkody w systemie, a w konsekwencji zaszkodzić instytucji.
- Przykłady:
  - Zagrożenie kradzieży zasobów, w tym informacji;
  - Niewłaściwe korzystanie z zasobów;
  - Wykorzystanie błędów.



# Elementy bezpieczeństwa

- Podatność (vulnerability) – to słabość lub luka w systemie przetwarzania danych, która może być wykorzystana przez zagrożenia, prowadząc do strat.

Szkoda występuje, gdy zagrożenie wykorzystuje podatność zasobu.





# Elementy bezpieczeństwa

- Incydent bezpieczeństwa (security incident)) – to niekorzystne zdarzenie, które można uznać za awarię, faktyczne lub domniemane naruszenie zasad ochrony informacji lub prawa własności.
- Przykłady:
  - Utrata poufności, integralności lub dostępności informacji,
  - Kradzież danych,
  - Zniszczenie informacji,
  - Błędne decyzje w oparciu o sfałszowane dane,
  - Blokada działania systemu.





# Elementy bezpieczeństwa

- Następstwa (impacts) – to wszelkie negatywne skutki incydentu dla instytucji.
- Przykłady:
  - Utrata określonej liczby klientów,
  - Straty w wyniku kradzieży sprzętu i oprogramowania,
  - Utrata przewagi konkurencyjnej,
  - Wyrok sądu,
  - Bankructwo z powodu utraty informacji,
  - Utrata zdrowia i życia osób,
  - Szkody dla otoczenia.



# Elementy bezpieczeństwa

- Ryzyko (risk) – prawdopodobieństwo albo możliwość, że określone zagrożenie wykorzysta podatność zasobu (lub grupy) aby spowodować naruszenie lub zniszczenie zasobów.
- Zabezpieczenie (sefeguard) – to praktyka, procedura lub mechanizm redukujący ryzyko do pewnego akceptowanego poziomu – ryzyka szczątkowego (residual risk).



# Elementy bezpieczeństwa

- Zabezpieczenie powinno realizować przynajmniej jedną z funkcji:
  - Ochronę przed zagrożeniami,
  - Odstraszanie intruzów,
  - Ograniczanie wpływu podatności,
  - Ograniczanie następstw,
  - Wykrywanie niepożądanych incydentów, zapobieganie im,
  - Ułatwianie odtwarzania naruszonych zasobów.



# Elementy bezpieczeństwa

- Analiza ryzyka (risk analysis) –to proces identyfikacji ryzyka, określenia jego źródeł, wielkości i wyodrębniania obszarów wymagających zabezpieczeń.
- Scenariusz ryzyka (risk scenario) –pokazuje, w jaki sposób dane zagrożenie (grupa) może wykorzystać podatności



# Elementy bezpieczeństwa

- Ocena ryzyka (risk evaluation) – porównanie szacowanego ryzyka z założonymi kryteriami ryzyka w celu wyznaczenia powagi ryzyka.
- Oszacowanie ryzyka (risk assessment) – proces oceny znanych i postulowanych zagrożeń oraz podatności, przeprowadzony w celu określenia potencjalnych strat i ustalenie poziomu akceptowalności działania systemu.



# Elementy bezpieczeństwa

- Zarządzanie ryzykiem (risk management) –to całkowity proces identyfikacji monitorowania oraz eliminowania / minimalizowania prawdopodobieństwa zaistnienia zdarzeń, które mogą mieć wpływ na zasoby systemu.
- Postępowanie z ryzykiem (risk treatment) – wybór i wdrożenie środków wpływających na zmianę wielkości ryzyka.



# Elementy bezpieczeństwa

- Ocena ryzyka (risk evaluation) – porównanie szacowanego ryzyka z założonymi kryteriami ryzyka w celu wyznaczenia powagi ryzyka.
- Akceptacja ryzyka (risk acceptance) – decyzja zarządu, dopuszczająca pewien zidentyfikowany stopień ryzyka (wynikająca najczęściej z przyczyn ekonomicznych lub technicznych).





# Identyfikacja i uwierzytelnianie

- Hasła jednorazowe
- Protokół challenge-response
- Protokół Fiata-Shamira



# Hasła jednorazowe

- Wygenerowanie losowego ciągu  $C_0$ .  
Wyznaczenie kolejnych ciągów  
 $C_{n+1} = f(C_n)$ ,  $n = 0 \dots m$
- Przekazanie użytkownikowi ciągów  $C_1 \dots C_m$
- Zniszczenie w systemie wszystkich wygenerowanych ciągów, oprócz ostatniego  $C_{m+1}$



# Hasła jednorazowe

- Funkcja  $f$  musi spełniać dwa warunki
  - nie istnieje praktyczna możliwość wyznaczenia różnych  $x_1$  oraz  $x_2$  takich, że  $f(x_1) = f(x_2)$
  - nie istnieje praktyczna możliwość wyznaczenia elementu  $x$  na podstawie wartości  $f(x)$



# Etap uwierzytelniania

- Użytkownik przekazuje do systemu ciąg  $C_m$
- W systemie następuje sprawdzenie, czy  $C_{m+1}=f(C_m)$   
Jeżeli warunek jest spełniony, to identyfikacja jest zakończona, a nowym wzorcem w systemie staje się  $C_m$
- Użytkownik usuwa wykorzystany ciąg



# Protokół challenge-response z kluczem tajnym

- **A** i **B** posiadają ten sam tajny klucz  $K$  i ustalili jakiej funkcji szyfrującej  $H$  będą używać
- **A** przedstawia się **B**: jestem **A**
- **B** losuje liczbę  $r$  i przesyła do **A**
- **A** oblicza  $H(K, r)$  i przesyła do **B**
- **B** również oblicza  $H(K, r)$  i porównuje z wartością otrzymaną od **A**



# Protokół challenge-response z kluczem publicznym

- **A** posiada klucz prywatny  $K_{\text{prywatny}}$  i opublikował  $K_{\text{publiczny}}$ . **A** i **B** używają tej samej funkcji szyfrującej  $H$
- **A** przedstawia się **B**: jestem **A**
- **B** losuje liczbę  $r$  i przesyła do **A**
- **A** szyfruje  $r$   $r' = H(K_{\text{prywatny}}, r)$  i przesyła do **B**
- **B** oblicza  $H(K_{\text{publiczny}}, r')$  i otrzymuje  $r$



# Protokół Fiata-Shamira

- Rejestracja użytkownika
  - **A** wybiera losowo dwie duże liczby pierwsze  $p$  i  $q$  oraz oblicza  $n=pq$ .
  - Użytkownik **A** wybiera  $s$ , względnie pierwszą z  $n$ . Wartość  $s$  pozostaje znana wyłącznie użytkownikowi (klucz prywatny).
  - **A** publikuje wartość  $n$  oraz  $v=s^2 \bmod n$  (klucz publiczny)



# Protokół Fiata-Shamira

- Weryfikacja
  - **A** wybiera liczbę  $k$ , względnie pierwszą z  $n$ , a następnie oblicza  $x = k^2 \bmod n$ . Wartość  $x$  przesyła do **B**.
  - **B** wysyła do **A**  $b = 0$  lub  $1$ .
  - **A** oblicza  $y = ks^b \bmod n$ . Wartość  $y$  przesyła do **B**  
[ $y = k$ , dla  $b = 0$ ;  $y = k * s \bmod n$ , dla  $b = 1$ ]
  - **B** sprawdza czy  $y^2 = v^b k^2 \bmod n$   
[ $y = k^2 \bmod n$ , dla  $b = 0$ ;  $y^2 = x * v \bmod n$ , dla  $b = 1$ ]





# Protokół Fiata-Shamira

- Rejestracja
  - $p=31$ ;  $q=61$  TAJNE
  - $n=p \cdot q=1891$
  - $s=23$  KLUCZ PRYWATNY
  - $v=s^2 \bmod n=529$  KLUCZ PUBLICZNY



# Protokół Fiata-Shamira

- Test (**A** udowadnia **B**, że zna klucz prywatny)
  - **A** wybiera  $k$  względnie pierwsze z  $n$   $k=29$
  - **A** wysyła **B**  $x=k^2 \bmod n = 841$
  - **B** wysyła do **A**  $b$   $b=0$   $b=1$
  - **A** wysyła do **B**  $y=ks^b \bmod n = 29$   $667$
  - **B** weryfikuje odpowiedź
  - $v^b k^2 \bmod n$   $841$   $444889$
  - $y^2$   $841$   $444889$



# Szyfrowanie

- Szyfr Cezara
- Szyfr Vigenere'a, Enigma
- Zasada Kerckhoffs'a
- Szyfry symetryczne
- Szyfry asymetryczne



# Szyfrowanie

Szyfrowanie jest użyteczne, kiedy

- nakłady finansowe, które należałoby ponieść na złamanie szyfru przekraczają w sposób zdecydowany wartość chronionej informacji;
- czas potrzebny na odkrycie informacji jest dłuższy niż czas, po upływie którego informacja traci swoją wartość.



# Szyfrowanie

Szyfrować można

- pojedyncze pliki
- systemy plikowe
- transmisję



# Proste szyfry

## Szyfr Cezara

- $S = (n + k) \bmod d$
- $n$  – numer znaku,  $k$  – przesunięcie,  $d$  – rozmiar alfabetu
- Błb nb lpub

## Podstawienia

- d! rozwiązań, prosty do złamania

# Szyfr Vigenere'a

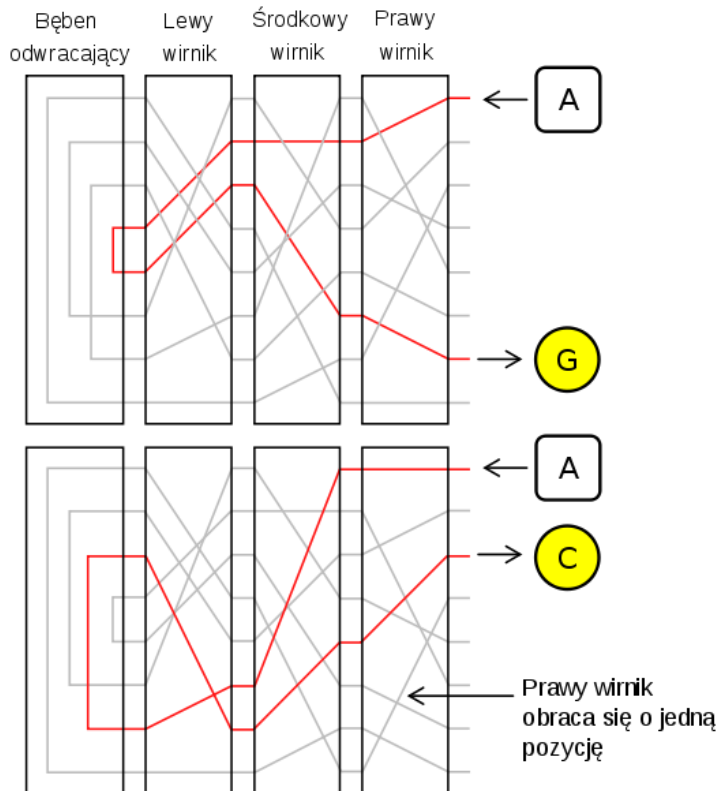
- $s_i = p_i \text{ XOR } k_i$
- $s_i$  - i-ty znak tekstu zaszyfrowanego
- $p_i$  - i-ty znak tekstu szyfrowanego
- $k_i$  - i-ty znak klucza

	a	b	c	d	e	f	g	h	i	j	k	l	m	...	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M		Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N		A
c	C	D	E	F	G	H	I	J	K	L	M	N	O		B

- klucz: cb, tekst jawny ela, zaszyfrowany GMC

# Enigma

- Praktyczne zastosowanie szyfru Vigenere'a



Wikipedia Commons

Bezpieczeństwo danych





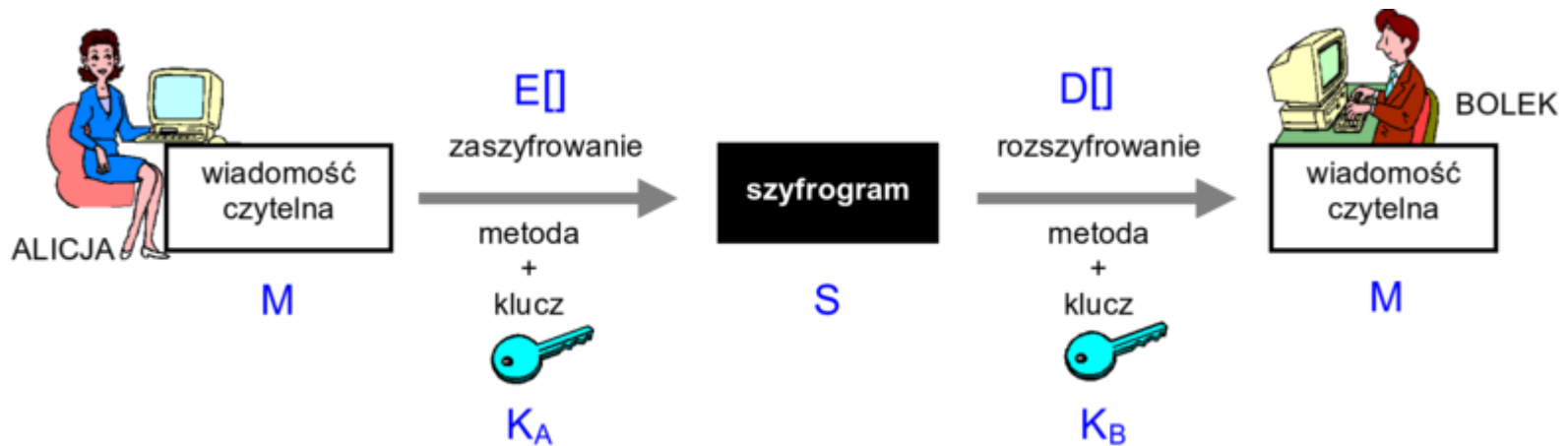
# Zasada Kerckhoffsza

- Zgodnie z tą zasadą, algorytm może być, a nawet z wielu względów powinien być publicznie znany. Przemawia za tym ułatwienie publicznej oceny i dyskusji jakości, jakie potencjalnie oferuje powszechna dostępność każdego nowo-opracowanego algorytmu dla światowej rzeszy kryptoanalityków. Dzięki temu, łatwiej i wcześniej można wykryć ewentualne luki w koncepcji algorytmu bądź w samej jego konstrukcji.



# Szyfrowanie z kluczem

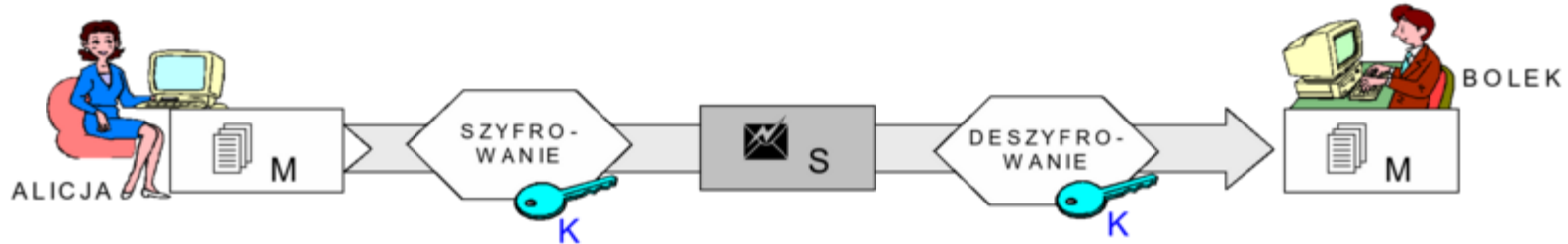
- $E_{KA}[M]=S \rightarrow S \rightarrow D_{KB}[S]=M$



<http://wazniak.mimuw.edu.pl/index.php?title=Grafika:Bsi-w-04-03.png>

# Szyfry symetryczne

- Wykorzystują klucz tajny
- $E_K[M]=S \rightarrow S \rightarrow D_K[S]=M$
- Przykładowe algorytmy: DES, 3DES, AES



<http://wazniak.mimuw.edu.pl/index.php?title=Grafika:Bsi-w-04-05.png>



# Szyfry symetryczne

- tożsamość problemu poufności wiadomości z problemem tajności klucza
  - wiadomość jest bezpieczna dopóki osoba trzecia nie pozna tajnego klucza  $K$
- problem dystrybucji klucza
  - jak uzgodnić wspólny klucz bez osób trzecich, będąc oddalonym o setki, a nawet tysiące kilometrów?





# Szyfry symetryczne

- problem skalowalności
  - dla 2 komunikujących się w systemie osób wymagane jest przechowywanie przez każdą z nich 1 klucza; dla 3 osób - 3 kluczy (przez każdą osobę); 4 os. = 6 kluczy; 10 os. = 45 kluczy; 100 os. = 4950 kluczy; ...
- autentyczność
  - tajność klucza nie zapewnia autentyczności - nie można wykazać formalnie która z dwóch stron jest rzeczywistym nadawcą wiadomości, skoro obie posługują się tym samym kluczem.





# DES

- Algorytm DES pracuje na 64-bitowych blokach tekstu jawnego, co odpowiada 8 znakom 8-bitowego kodu ASCII. Klucz składa się z 64 bitów, przy czym 8 z nich jest bitami parzystości. Zatem w istocie, w trakcie wyboru klucza można określić jedynie 56 bitów.

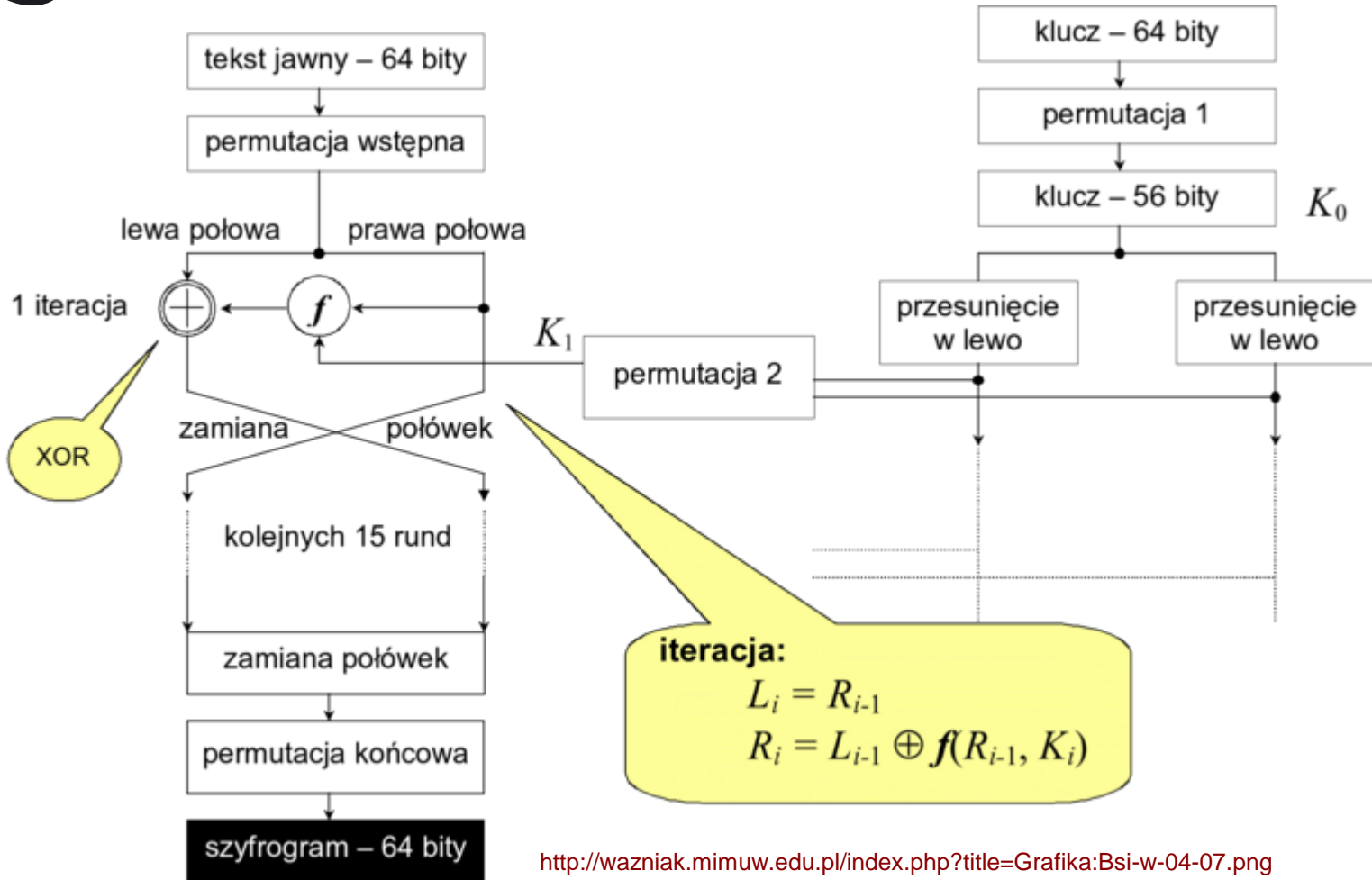


# DES

Algorytm działa w kilku etapach nazywanych fazami:

- wstępna permutacja wejściowego bloku danych (na podstawie tabeli transpozycji)
- podział bloku na lewą i prawą połowę o długości 32 bitów
- 16 jednakowych cykli operacji podstawiania i przestawiania wykorzystujących pewną funkcję  $f$ , w czasie których dane zostają połączone z kluczem
- połączenie lewej i prawej połowy bloku
- permutacja końcowa (odwrotność permutacji wstępnej)

# DES



<http://wazniak.mimuw.edu.pl/index.php?title=Grafika:Bsi-w-04-07.png>





# DES

- Celem permutacji wstępnej i końcowej było spowolnienie softwarowych implementacji algorytmu
- Każda kolejna runda, dokonuje takich samych obliczeń na wynikach obliczeń z poprzedniej rundy i specjalnym podkluczu  $K_i$  generowanym z 56b klucza  $K_0$ .



# DES

- Generacja podkluczy:
  - 56 bitów klucza dzielone jest na dwie połowy po 28 bitów
  - w każdej iteracji bity obu połówek są cyklicznie przesuwane w lewo o jeden lub dwa bity, w zależności od numeru iteracji
  - ostatecznie wykonywana jest permutacja kompresująca, dzięki której z 56b klucza, otrzymujemy 48b podklucz  $K_i$  używany w funkcji  $f$



# DES

- Funkcja  $f$ 
  - prawa połowa  $R_{i-1}$  rozszerzana jest z 32 bitów do 48 bitów za pomocą permutacji rozszerzonej (e-blok) i sumowana mod 2 z 48 bitami podklucza  $K_i$  danego cyklu
  - otrzymany wynik poddawany jest operacji podstawienia poprzez wykorzystanie bloków podstawień (S-bloki):
    - ciąg 48 bitów dzielony jest na 8 bloków po 6 bitów
    - każdy ciąg 6 bitów jest redukowany do 4 bitów funkcją podstawienia
    - otrzymany 32b ciąg poddawany jest permutacji zwykłej
    - oraz sumowany mod 2 z lewą połową  $L_{i-1}$  bloku wejściowego

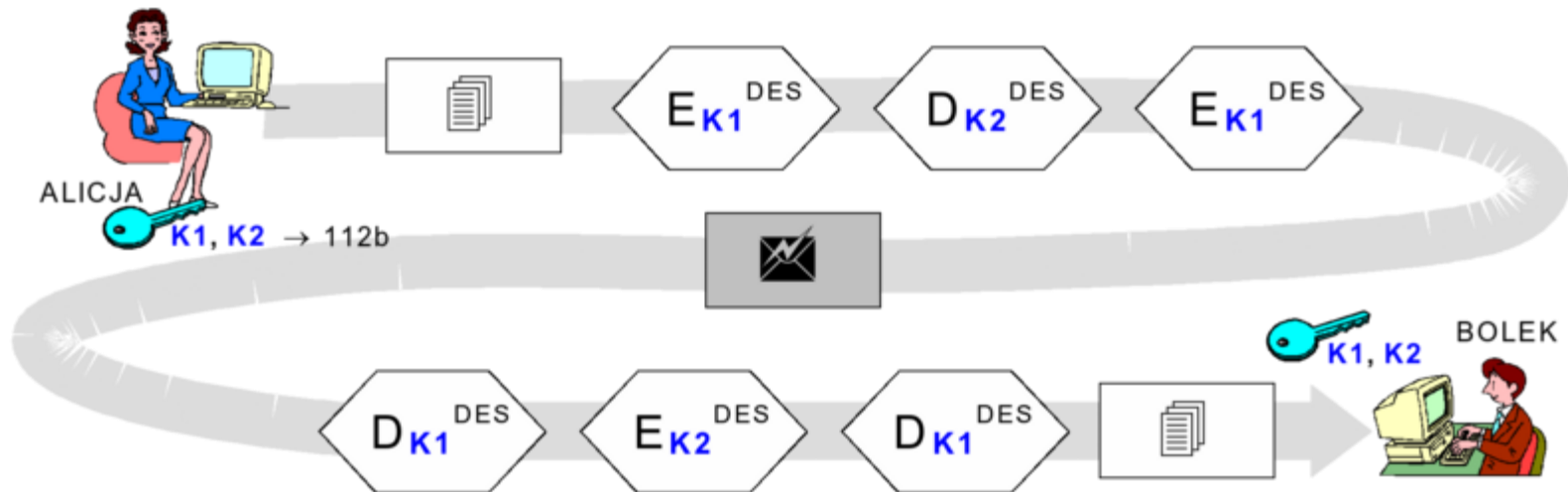
# 3DES

Czas złamania algorytmu DES:

1977 rok – jeden dzień (maszyna 20mln\$)

1993 rok – 7 godzin (maszyna 1mln\$)

1998 rok – 2 dni (maszyna 250000\$)





# Algorytm AES

- Odmiana algorytmu Rijndael z 1999 roku
- Może używać 128, 192 lub 256 – bit klucza
- W 2003 roku rząd USA zatwierdził AES-128, AES-192, AES-256 jako narzędzie do kodowania materiałów rządowych z klauzulą SECRET, a AES-192, AES-256 jako narzędzia do kodowania materiałów rządowych z klauzulą TOP SECRET
- W 2010 roku Intel wypuścił na rynek procesory z rozkazami AVX ułatwiającymi implementację AES





# AES

- Fazy algorytmu:
  - I. Transformacja klucza "AddRoundKey,,
  - II. Nr-1 rund składających się z:
    - Transformacja SubBytes
    - Transformacja ShiftRows
    - Transformacja MixColumns
    - Transformacja AddRoundKey
  - III. Runda finałowa składająca się z:
    - Transformacja SubBytes
    - Transformacja ShiftRows
    - Transformacja AddRoundKey





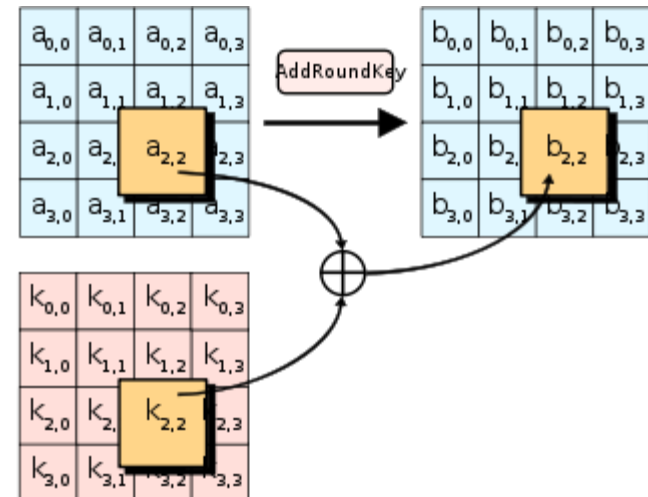
# AES

- Odmiany AES

	Liczba kolumn	Liczba iteracji
Wariant	Nk	Nr
AES-128	4	10
AES-192	6	12
AES-256	8	14

# AES

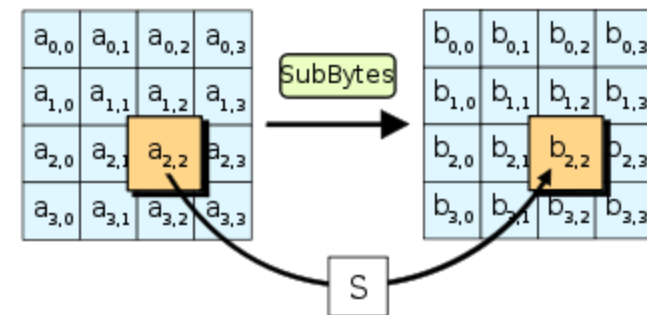
- AddRoundKey
  - Operacja AddRoundKey polega na wykonaniu operacji XOR w każdej rundzie pomiędzy całym blokiem a kluczem rundy





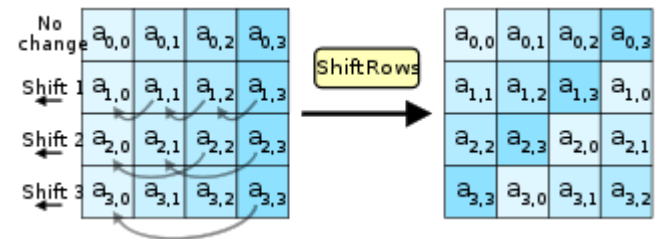
# AES

- SubBytes
  - Transformacja „podstawienie bajtów” (substitute bytes) operuje na każdym bajcie stanu niezależnie i zmienia wartość tego bajtu.



# AES

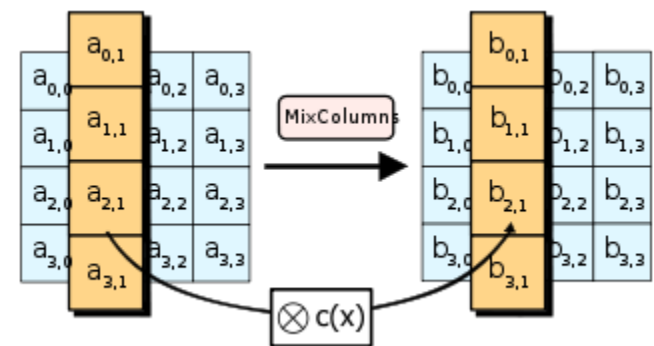
- Shift Rows
  - Transformacja ShiftRows przesuwają cyklicznie bajty w 3 dolnych wierszach macierzy stanu. Wiersze 2,3 i 4 są przesuwane cyklicznie o 1, 2 i 3 bajty



# AES

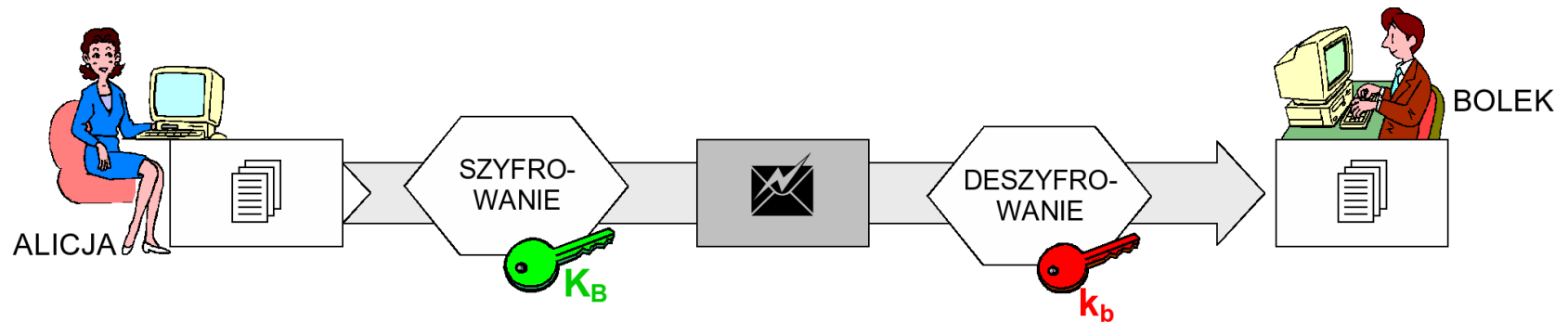
- MixColumns

- Operacja ta polega na przemnożeniu wielomianu utworzonego z bajtów kolumny
- np.  $W(X) = s_{0,0} * x^3 + s_{1,0} * x^2 + s_{2,0} * x^1 + s_{3,0}$
- przez stały wielomian:  $C(X) = 3 * x^3 + 1 * x^2 + 1 * x^1 + 2$
- Mnożenie to wykonywane jest modulo  $X^4+1$



# Szyfry asymetryczne

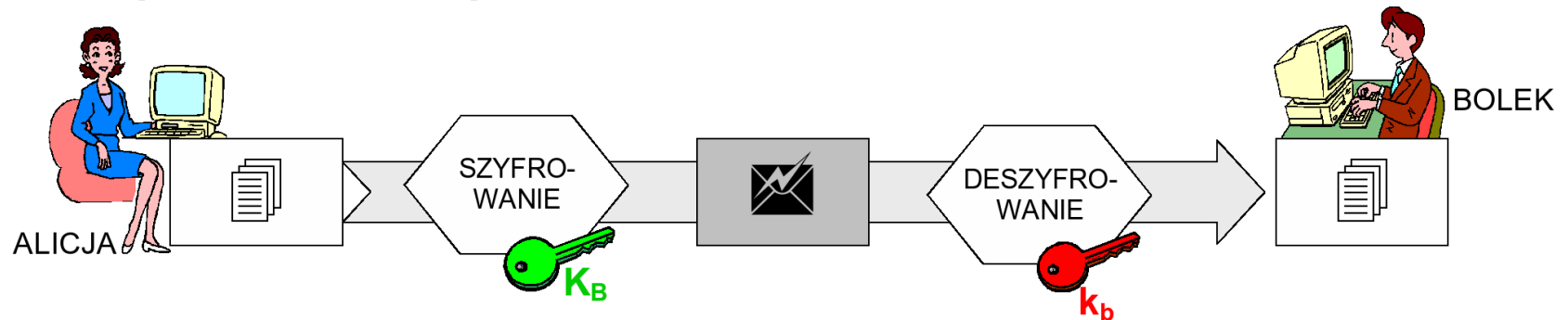
- Wykorzystują klucz jawny i klucz prywatny
- Przykład: RSA



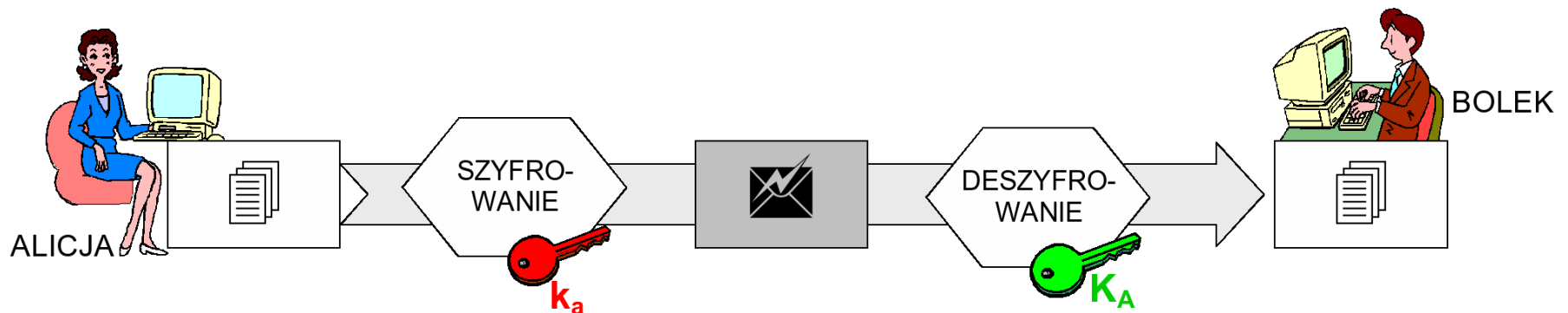
<http://wazniak.mimuw.edu.pl/images/a/a0/Bsi-w-04-12.png>

# Szyfry asymetryczne

- Zapewnienie poufności



- Zapewnienie autentyczności





# RSA

1. Wybieramy dwie liczby pierwsze  $P$  i  $Q$ . Niech  $P=11$  i  $Q=3$ . Liczby  $P$  i  $Q$  nie są publikowane.
2. Obliczamy iloczyn  $N=P*Q$ .  $N=11*3=33$ . Liczba  $N$  jest jawna.
3. Obliczamy wartość  $F=(P-1)*(Q-1)$ .  
 $F=(11-1)*(3-1)=20$ . Liczby  $P$  i  $Q$  nie są już potrzebne i można je skasować.



# RSA

4. Wybieramy taką liczbę  $E$ , która jest mniejsza od  $F$  i względnie z nią pierwsza. Dla przyjętych danych przyjmujemy  $E=17$ . Para liczb  $\{E, N\}$ , a więc  $\{17, 33\}$  stanowi klucz publiczny.
5. Obliczamy liczbę  $D$ , która musi być mniejsza od  $F$  oraz spełniać warunek, że reszta dzielenia iloczynu  $D \cdot E$  przez  $F$  musi być równa 1. Dla przyjętych danych tylko  $D=13$  spełnia oba warunki.  $D$  nie jest publikowana i współtworzy klucz prywatny  $\{D, N\} - \{13, 33\}$ .



# RSA szyfrowanie

- Szyfrowanie  $S = M^E \pmod{N}$ 
  - Klucz publiczny  $\{E, N\} = \{17, 33\}$ , znak  $M=5$
  - $S = 5^{17} \pmod{33} = 762939453125 \pmod{33} = 14$
- Deszyfrowanie  $M = S^D \pmod{N}$ 
  - Klucz prywatny  $\{D, N\} = \{13, 33\}$
  - $S = 14^{13} \pmod{33} = 793714773254144 \pmod{33} = 5$
- W praktyce  $N = 10^{150} - 10^{200}$





# Potwierdzanie autentyczności

- Funkcja skrótu
- Potwierdzanie integralności
- Podpis cyfrowy
- Niezaprzeczalność



# Potwierdzanie autentyczności

- Metoda 1:
  - szyfrujemy całą wiadomość kluczem prywatnym nadawcy
  - koszt obliczeń rośnie z wielkością wiadomości
- Metoda 2:
  - tworzymy skrót wiadomości o ustalonym z góry rozmiarze  $n$
  - szyfrujemy kluczem prywatnym nadawcy tylko skrót
  - koszt mały -  $n$  małe
  - koszt stały - nie rośnie z wielkością wiadomości i zależy tylko od  $n$



# Funkcja skrótu, własności

- kompresja: że rozmiar skrótu musi być mniejszy od rozmiaru samej wiadomości
- łatwość obliczeń: czas wielomianowy wyznaczenia dla dowolnego  $h[M]$  dla dowolnego  $M$
- odporność na **podmianę** argumentu: dla danego  $h[M]$  obliczeniowo trudne znalezienie takiego  $M'$ , że  $h[M]=h[M']$
- odporności na **kolizje**: obliczeniowo trudne znalezienie dwóch dowolnych argumentów  $M \neq M'$  takiego, że  $h[M]=h[M']$

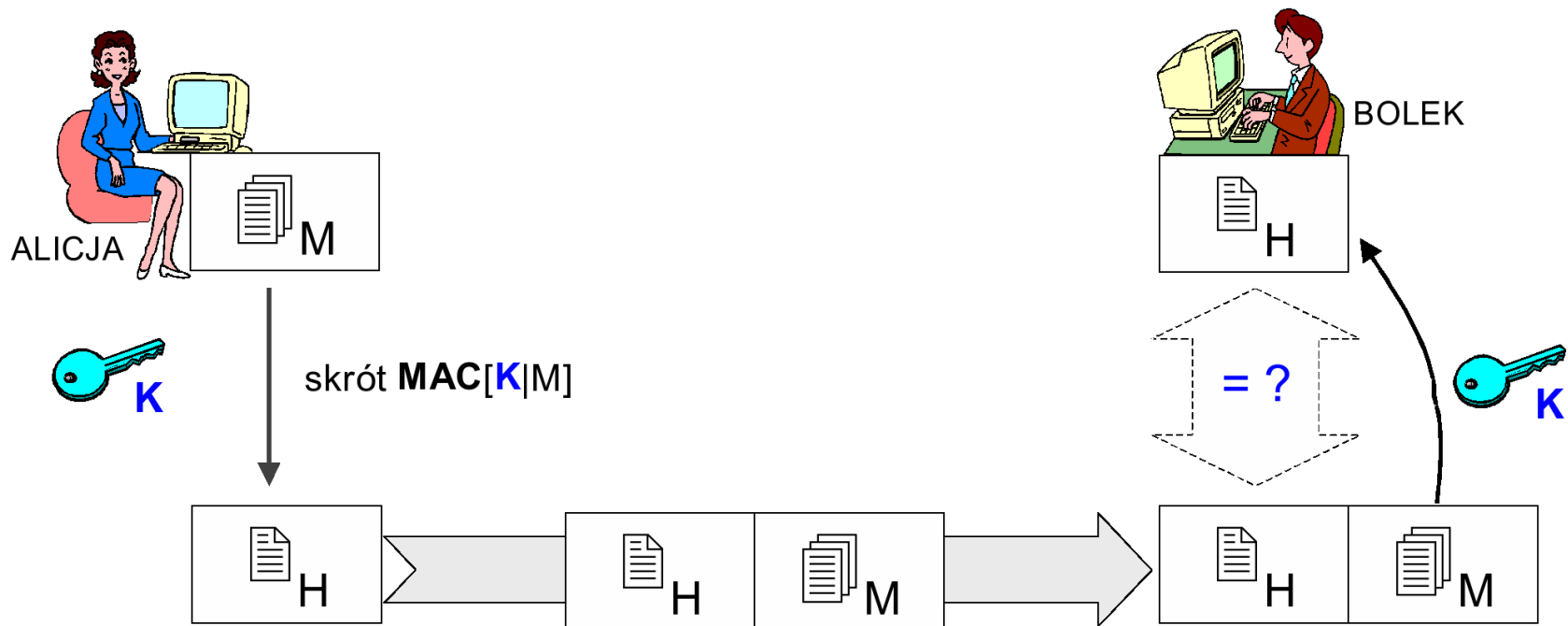




# Zastosowania funkcji skrótu

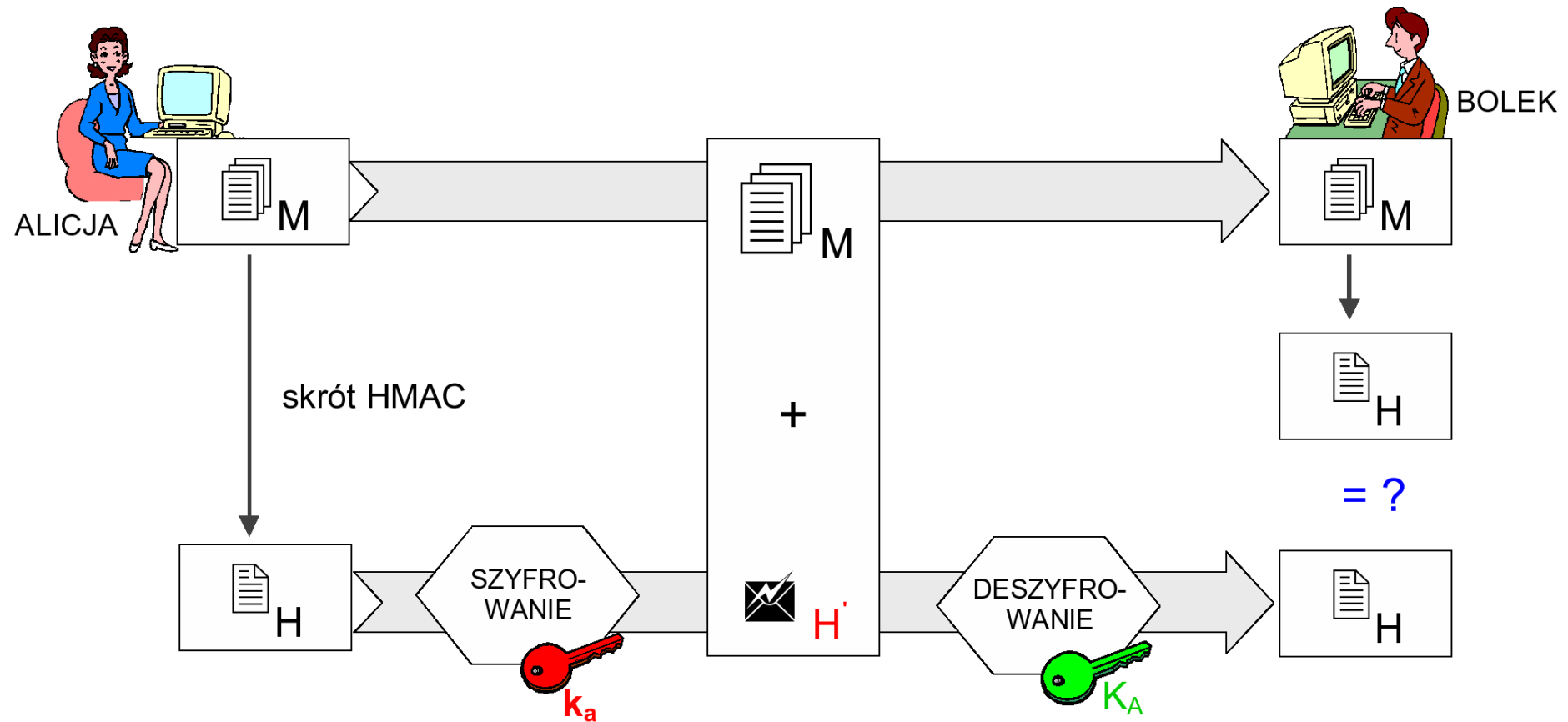
- zapewnienie integralności wiadomości bez klucza kryptograficznego
- zapewnienie integralności oraz autentyczności wiadomości: **MAC** - *message authentication code* (z kluczem kryptograficznym)

# Zapewnienie integralności



<http://wazniak.mimuw.edu.pl/images/e/ef/Bsi-w-05-01.png>

# Podpis cyfrowy



<http://wazniak.mimuw.edu.pl/images/3/38/Bsi-w-05-02.png>



# Usługa niezaprzeczalności

Podpisy elektroniczne wg dyrektywy Unii Europejskiej 1999/93/EC :

- Zwykłe podpisy
- Zaawansowane (bezpieczne) podpisy elektroniczne
- Kwalifikowane podpisy elektroniczne



# Usługa niezaprzeczalności

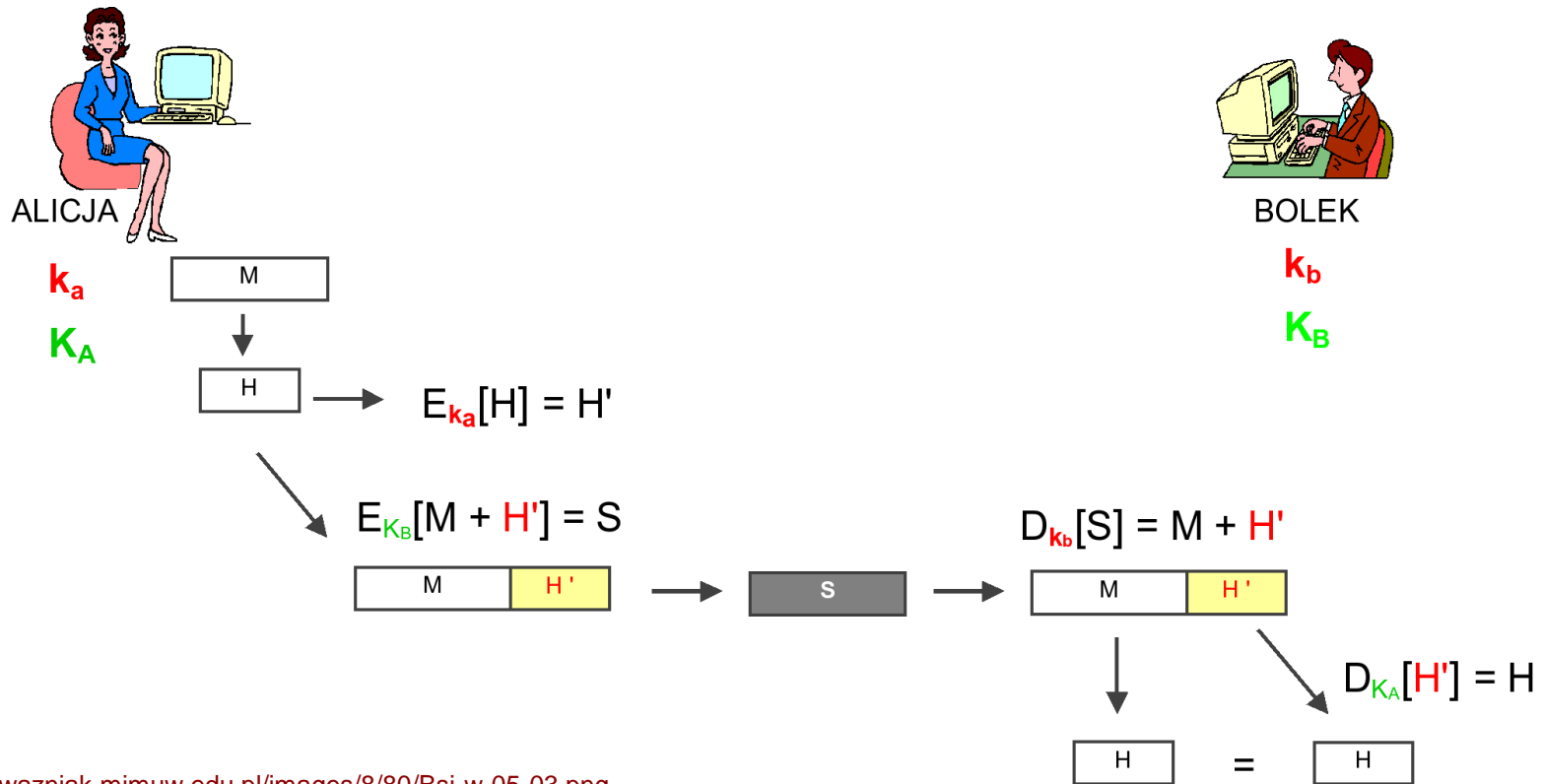
Podpisy elektroniczne mogą funkcjonować niezależnie od dokumentów (magazynowanie, przesyłanie).

Dodatkowo podpisy zaawansowane i kwalifikowane:

- są zależne od treści komunikatu,
- dotyczą całego dokumentu.



# Poufność + autentyczność + nienaruszalność



<http://wazniak.mimuw.edu.pl/images/8/80/Bsi-w-05-03.png>