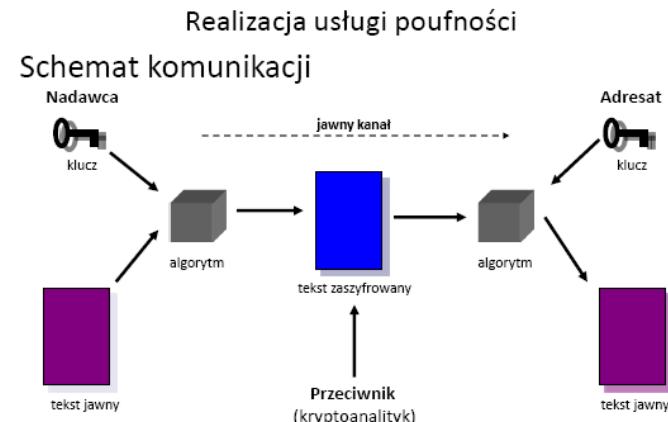


WKR – Odpowiedzi na pytania

1.) Zasada Kerchoffa

Algorytmy kryptograficzne są jawne, natomiast ich bezpieczeństwo opiera się na tajności kluczy. Warunkiem koniecznym (ale nie dostatecznym) bezpieczeństwa szyfru jest duża liczba możliwych kluczy.

2.) Usługi: poufność, integralność



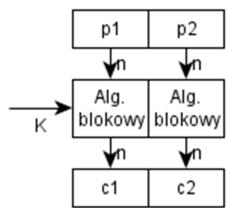
Usługa poufności służy uniemożliwieniu osobom trzecim zrozumienie treści wiadomości wysyłanej między nadawcą a odbiorcą. W tym celu wykorzystuje się algorytmy symetryczne (do szyfrowania i deszyfrowania używany jest ten sam klucz). Przykłady: szyfr Cezara, szyfr Vernama, szyfr Vigenere'a) i asymetryczne (do szyfrowania i deszyfrowania używane są różne klucze). Przykład: szyfr z kluczem publicznym i prywatnym).

Usługa integralności służy do zapewnienia, aby odbiorca otrzymał dokładnie taką wiadomość, jaką wysłał nadawca. Ma na celu wykrycie ewentualnych modyfikacji wiadomości przez przeciwnika lub wykrycie błędów transmisji jawnym kanałem. W tym celu wykorzystuje się funkcje skrótu i podpis cyfrowy.

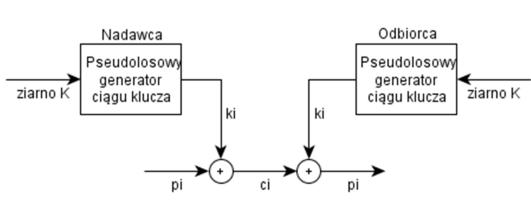
3.) Szyfry symetryczne (tajnego klucza, problem dystrybucji kluczy)

Kryptosystemy symetryczne (inaczej systemy tajnego klucza) – możliwość szyfrowania równoważna możliwości deszyfrowania. Klucz k stosowany przez strony A i B odpowiednio do szyfrowania i deszyfrowania jest kluczem tajnym. Problem dystrybucji kluczy polega na tym, że strona A i B muszą być zaopatrzone w odpowiednią liczbę tajnych kluczy, które muszą być dostarczone do obu stron w sposób bezpieczny.

4.) Klasifikacja: szyfry blokowe i strumieniowe



Szyfr blokowy – tekst jawny dzielony jest na bloki o ustalonej długości, a następnie szyfrowany blok po bloku. Na podstawie zadanego klucza przekształca wejściowy blok danych w inny blok w taki sposób, że niemożliwe jest odwrócenie tego przekształcenia, czyli odzyskanie bloku wejściowego na podstawie bloku wyjściowego bez znajomości klucza. Przykład szyfru blokowego: DES, 3DES, AES.



Szyfr strumieniowy – tekst jawny jest dzielony na pojedyncze znaki lub bity, a następnie każdy ten element jest szyfrowany kluczem należącym do strumienia kluczy. W szyfrze Vernama dodano ograniczenie, że klucz ma być nieokresowym, losowym strumieniem bitów nie krótszym od tekstu jawnego, który jest szyfrowany.

5.) Szyfrem z kluczem jednokrotnym (warunki 1-3)

Szyfr z kluczem jednokrotnym (inaczej szyfr Vernama) podlega następującym ograniczeniom, jeśli chodzi o klucz:

1. Klucz ma długość tekstu jawnego
2. Klucz jest losowym ciągiem znaków
3. Klucz jest stosowany tylko raz

Realizacja binarna szyfru Vernama:

- Test jawnny $p = p_1 \dots p_n$, $p_i \in \{0,1\}$, $i = 1, \dots, n$
- Klucz $k = k_1 \dots k_n$, $k_i \in \{0,1\}$, $i = 1, \dots, n$
- Szyfrogram $c = c_1 \dots c_n$,
- gdzie $c_i = p_i \oplus k_i$ dla $i = 1, \dots, n$
- Deszyfrowanie: $c_i \oplus k_i = p_i$
- Dowód: $c_i \oplus k_i = p_i \oplus k_i \oplus k_i = p_i \oplus 0 = p_i$

Szyfr Vernama jest bezwarunkowo bezpieczny tzn. nie można złamać szyfru niezależnie od posiadanych mocy obliczeniowych.

6.) Szyfr idealny. Twierdzenie Shannona

Twierdzenie Shannona – szyfr z kluczem jednokrotnym (inaczej szyfr Vernama) jest absolutnie bezpieczny, czyli jest to tzw. szyfr idealny.

Definicja szyfru idealnego: $\text{Prawd. } (m | c) = \text{Prawd. } (m)$,

gdzie m – wiadomość, c – szyfrogram.

To znaczy, że znajomość szyfrogramu nie daje żadnych informacji o tekście jawnym.

7.) Algorytm DES: budowa, bezpieczeństwo, 3DES

Algorytm DES należy do grupy szyfrów blokowych. Jego parametry to:

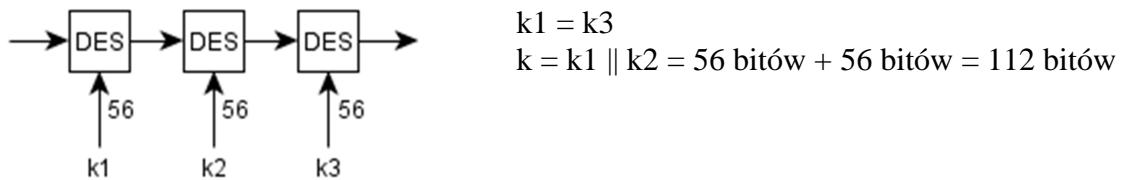
długość bloków: 64 bity długość klucza: 64 bity (faktyczna),
56 bitów (efektywna).

W algorytmie tym mieszane są przekształcenia różnego typu: podstawienia i permutacje (przestawienia). Wykonywane są one iteracyjnie, czyli wielokrotnie, gdzie liczba powtórzeń (rund) jest określona i równa 16.

Schemat ogólny:	Budowa schematu rundy:	Funkcja rundy f:	S-box:
	 + - szyfrowanie L1	 E – permutacja rozszerzająca 32-48 P – permutacja 32-32	 $S: \{0,1\}^6 \rightarrow \{0,1\}^4$

DES nie jest już uznawany za szyfr bezpieczny, ponieważ przeprowadzenie tzw. ataku brutalnego, czyli sprawdzenie wszystkich 2^{56} kluczy, zajmuje rozsądnią ilość czasu ze względu na obecną moc obliczeniową komputerów.

3DES jest próbą ratowania algorytmu DES. Zgodnie ze swoją nazwą, w algorytmie tym wykorzystuje się trzykrotnie algorytm DES, ale tylko z dwoma różnymi kluczami.



8.) AES – ogólnie, parametry

AES – następna DES-a, również należący do grupy szyfrów blokowych. Jego parametry to:
 długość bloków: 128 bitów długość klucza: 128, 192 lub 256 bitów

9.) Usługa integralności danych

Dana jest funkcja skrótu h.

Krok 1: Nadawca oblicza skrót $h(M)$ dla wiadomości M.

Krok 2: Nadawca dołącza do M skrót $h(M)$.

Krok 3: Nadawca wysyła do odbiorcy wiadomość $M \parallel h(M)$

Odbiorca otrzymuje wiadomość $M' \parallel h(M)$ (założenie: skrót $h(M)$ dociera niezmieniony).

Krok 4: Odbiorca oblicza skrót otrzymanej wiadomości M' , czyli $h(M')$.

Krok 5: Odbiorca porównuje skróty $h(M)$ i $h(M')$. Jeśli $h(M) = h(M')$ to $M = M'$, a jeśli $h(M) \neq h(M')$ to $M \neq M'$.

10.) Definicja kryptograficznej funkcji skrótu (warunki 1-4, notacja matematyczna)

Funkcja skrótu h – notacja matematyczna:

$h: \{0,1\}^* \rightarrow \{0,1\}^n$ gdzie $\{0,1\}^*$ – zbiór wszystkich wiadomości o skończonej długości,
 $\{0,1\}^n$ – zbiór wszystkich wiadomości o długości n.

$M \in \{0,1\}^*$, $h(M) \in \{0,1\}^n$

Warunki nakładane na kryptograficzną funkcję skrótu:

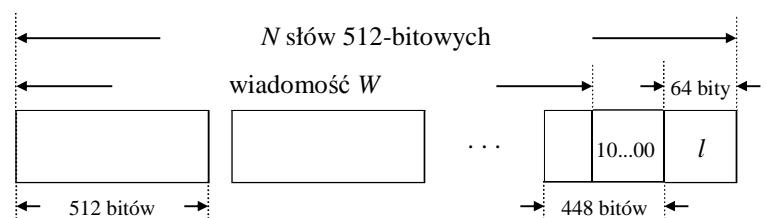
1. Obliczenie skrótu $h(M)$ jest „szybkie”
2. Dla danego h_0 znalezienie wiadomości M o tym samym skrócie ($h(M) = h_0$) jest trudne obliczeniowo. (Złożoność: 2^n).
3. Podrobienie skrótu wiadomości M jest trudne obliczeniowo tzn. dla danego M i $h(M)$ szukana jest $M' \neq M$ taka że $h(M) = h(M')$ (Złożoność: 2^n).
4. Funkcje skrótu są bezkolizyjne tzn. znalezienie pary wiadomości M i M' takich że $M \neq M'$, ale $h(M) = h(M')$ jest trudne (Złożoność: $2^{n/2}$).

11.) Funkcja skrótu MD4 – budowa

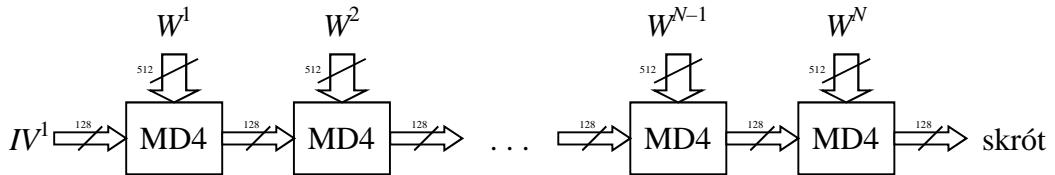
Wypełnianie wiadomości w MD4:

gdzie

$$l = (l_0, l_1) \text{ długość wiadomości mod } 2^{64}$$



Skracanie (wypełnionej) wiadomości W przez MD4



Schemat ogólny:	Budowa rundy:
<p>gdzie: $i = 1, 2, \dots, N$; $IV^i = \text{skróti}^{i-1}$; $\text{skróti}^0 = (IV_A^1, IV_B^1, IV_C^1, IV_D^1)$; $\text{skróti} = \text{MD4}(W) = \text{skróti}^N$</p>	<p>gdzie $j = 0, 1, \dots, 15$; $r = 1, 2, 3$</p>

Parametry MD4: skróty mają 128 bitów.

12.) Funkcje MD5, SHA1 – parametry, status bezpieczeństwa

MD5: skróty 128 bitów. Została złamana – udaje się znaleźć kolizje w rozsądny czasie. Jest nadal stosowana do zapewnienia usługi integralności, ale w podpisie cyfrowym już nie.

SHA1: skróty 160 bitów. Teoretyczne znajdowanie kolizji trwa 2^{80} . Ataki dedykowane (teoretyczne) trwają 2^{61} .