Kryptologia

Część 1

Wprowadzenie

Kryptografia a teoria informacji

Kontakt

dr hab. inż. Tomasz Hyla, prof. ZUT

Zachodniopomorski Uniwersytet Technologiczny,

Wydział Informatyki,

Katedra Inżynierii Oprogramowania i Cyberbezpieczeństwa,

Zespół Badawczy Ochrony Informacji, p.114 WI2

e-mail: *thyla@zut.edu.pl*

Microsoft Teams: Kryptologia N2 – zima 2022/2023

Wykład autorstwa: W. Chocianowicz, T. Hyla

Plan wykładu

1. Informacje o kursie
2. Podstawowe informacje o kryptologii
3. Zasady nowoczesnej kryptografii
4. Teoria informacji a kryptologia

ZASADY ZALICZENIA WYKŁADU

- Zaliczenie wykładu ma formę egzaminu pisemnego (forma bezpośrednia) albo ustnego (forma zdalna).
  - Na egzaminie nie będzie można korzystać z materiałów pomocniczych (notatek z wykładów, materiałów wykładowych, itp.), ani z urządzeń i mediów elektronicznych (kalkulatorów, smartfonów, internetu, itp.).

  - Egzamin będzie się składał z dwóch części:
  - testu wyboru,
  - problemów/zadań otwartych.

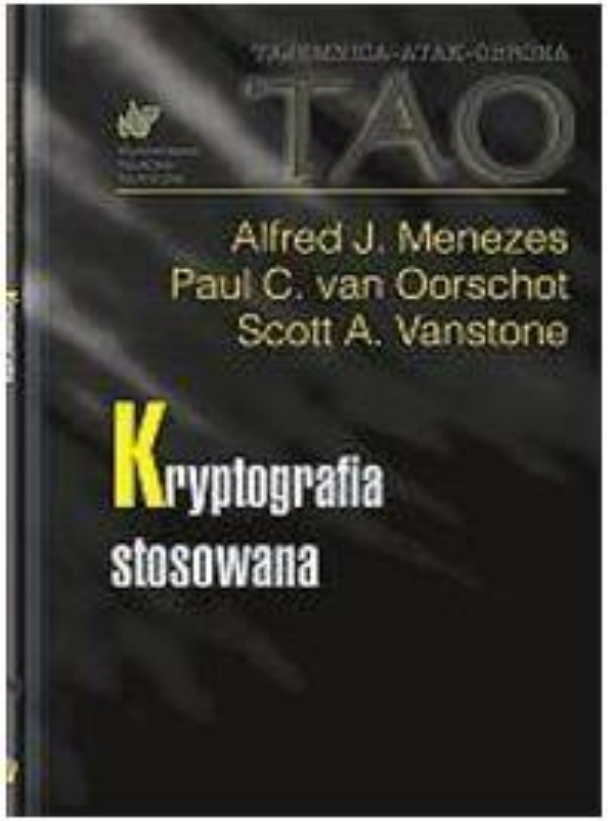
WYCIĄG Z SYLABUSA

T-W-1	Kryptografia a teoria informacji
T-W-2	Ogólne informacje o programowych bibliotekach kryptograficznych
T-W-3	Progowe metody podziału sekretów i obliczenia grupowe
T-W-4	Generowanie ciągów losowych o „dobrych" właściwościach kryptograficznych
T-W-5	Kryptografia bezkluczowa; zastosowania funkcji skrótu w różnych mechanizmach kryptograficznych
T-W-6	Kryptografia asymetryczna na krzywych eliptycznych
T-W-7	„Kryptografia wagi lekkiej" (Lightweight cryptography)
T-W-8	Ataki wykorzystujące fizyczną implementację algorytmów/mechanizmów kryptograficznych (side-channel attacks)
T-W-9	Kleptografia i kanały podprogowe/ukryte (subliminal/covert channels)
T-W-10	Protokoły o wiedzy zerowej
T-W-11	Kryptograficzne podstawy technologii „blockchain"
T-W-12	Pierścienie i ciała wielomianów
T-W-13	Kryptografia kwantowa i odporna na ataki kwantowe

Literatura podstawowa

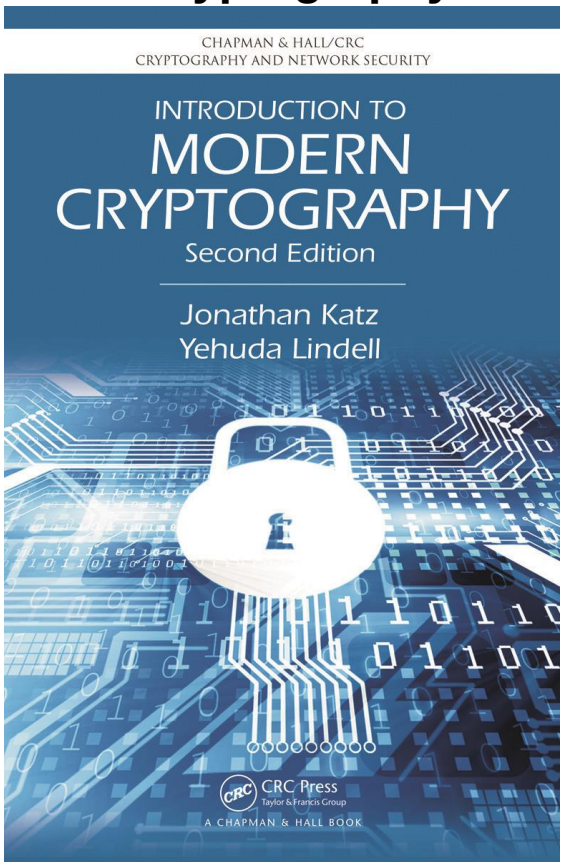
Alfred J.Menezes, Paul C.van Oorschot, Scott A.Vanstone

„Kryptografia stosowana”



Jonathan Katz, Yehuda Lindell,

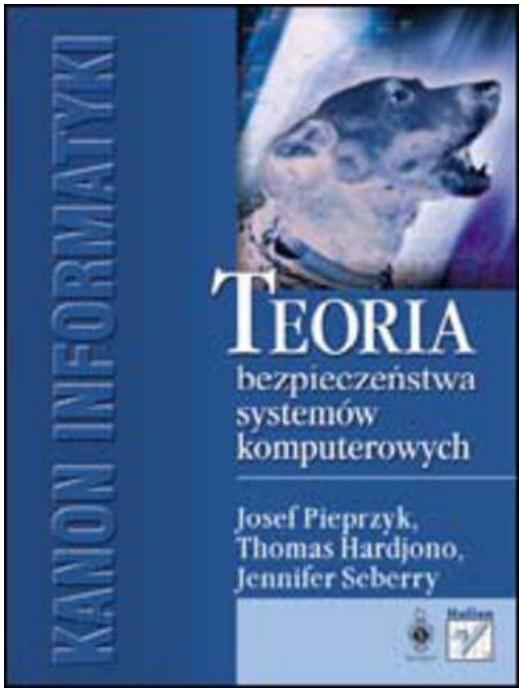
„Introduction to modern cryptography”



Literatura uzupełniająca

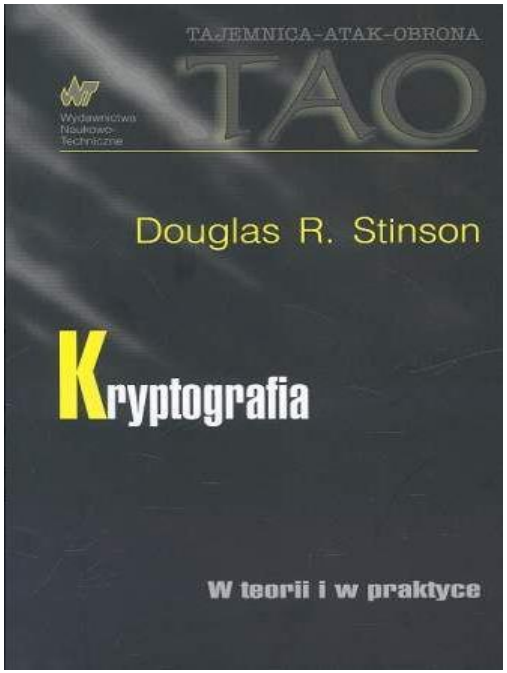
J.Pieprzyk, T.Hardjono, J.Seberry

„Teoria bezpieczeństwa systemów komputerowych”



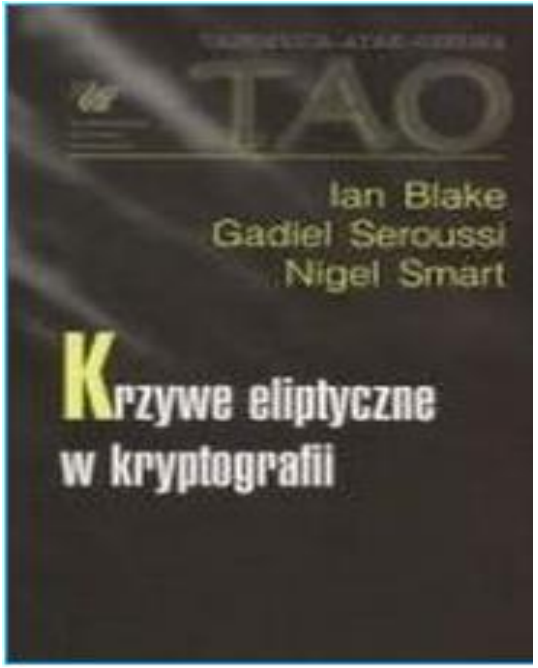
D.R.Stinson

„Kryptografia”



I.Blake, G.Seroussi, N.Smarti,

„Krzywe eliptyczne w kryptografii”



Plan wykładu

1. Informacje o kursie
2. Podstawowe informacje o kryptologii
3. Zasady nowoczesnej kryptografii
4. Teoria informacji a kryptologia

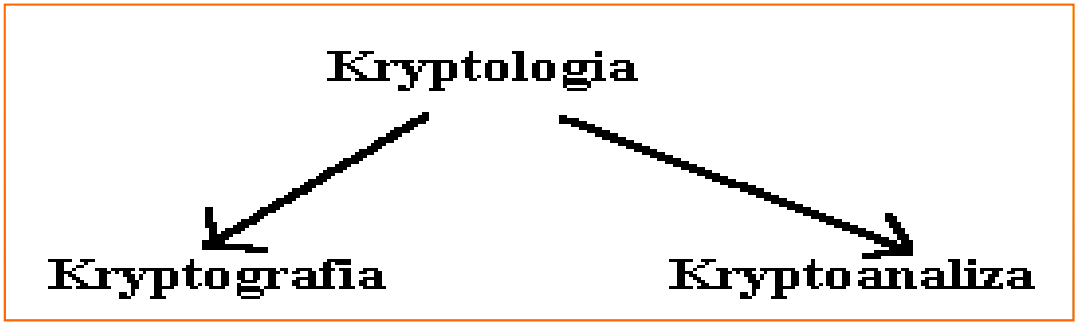
Czym jest Kryptografia?

- **definicja historyczna „the art of writing and solving codes” [Concise Oxford English Dictionary]**
- **definicja aktualna: „study of mathemtical techniques for securing digital information, systems, and distributed computations against adversarial attacks”**

- **Lata 70/80: z sztuki do dziedziny nauki i matematyki**

- **Główne zasady kryptografii:**
  1. **Centralna rola definicji**
  2. **Skupienie się na dokładnych założeniach**
  3. **Dowody bezpieczeństwa**

Przypomnienie



- **Kryptografia**

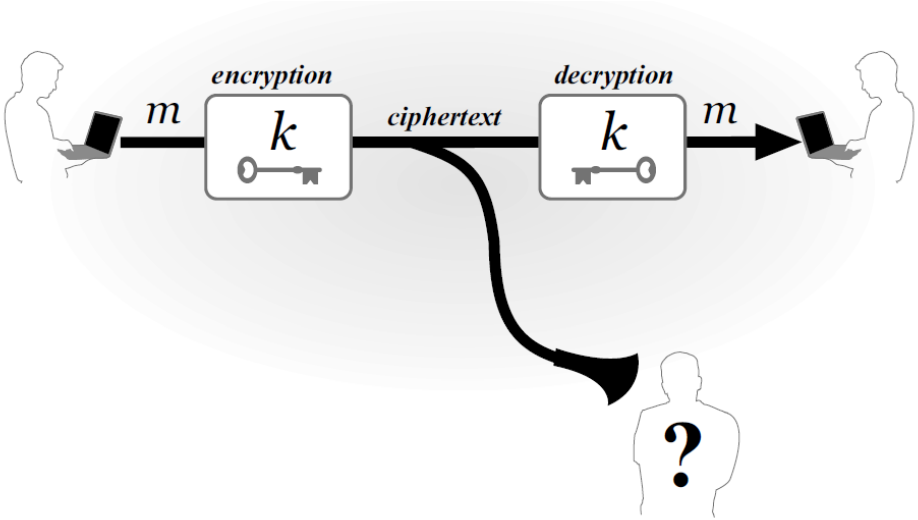
  Metody matematyczne realizacji usług poufności, integralności, uwierzytelniania (autentyczności i niezaprzeczalności).

- **Kryptoanaliza**

  Metody matematyczne przełamywania, osłabiania, pokonywania usług realizowanych metodami kryptograficznymi.

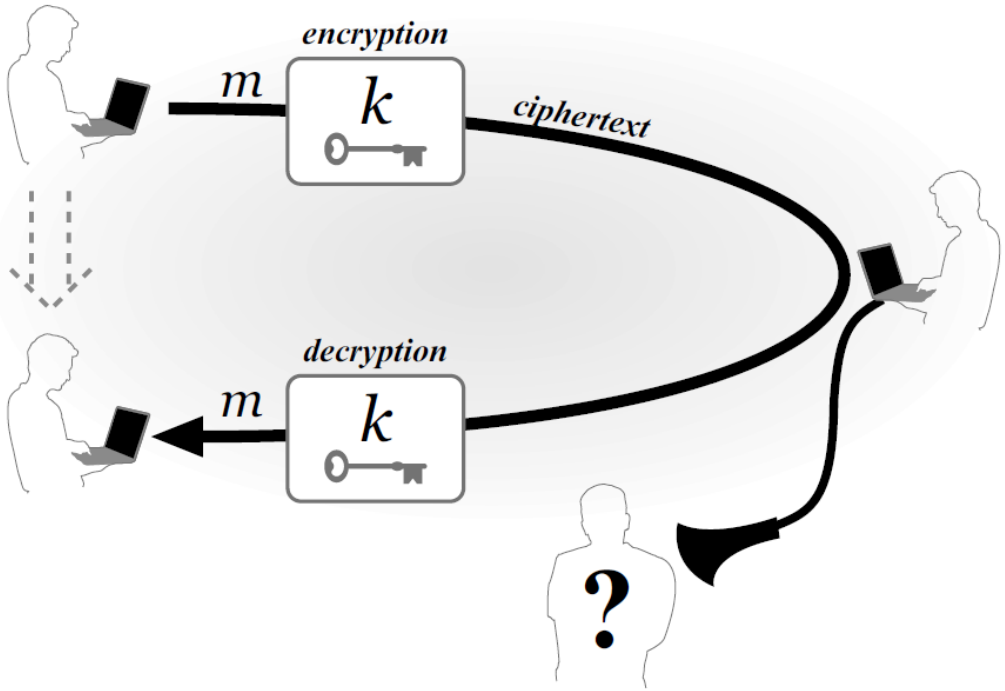
Szyfrowanie kluczem symetrycznym

- **Private-key (shared-key, secret-key) encryption**
- **Celem szyfrowania jest ukrycie tekstu jawnego przesyłanego pomiędzy dwoma stronami przed osobą podsłuchująca monitorującą kanał komunikacyjny**
- **Problem uzgodnienia klucza**



Szyfrowanie kluczem prywatnym symetrycznym

- **Czasami występuje tylko jedna strona, np. szyfrowanie dysku**
- **Problemem jest przechowywanie klucza**



Szyfrowanie kluczem symetrycznym

Konstrukcja systemu szyfrującego wymaga:
- **określenia przestrzeni wiadomości jawnych M;**
- **określenia przestrzeni wiadomości tajnych C;**
- **określenia przestrzeni kluczy K;**
- **określenia zbioru przekształceń szyfrujących $\{E_e : e \in K\}$;**
- **określenia odpowiedniego zbioru przekształceń deszyfrujących $\{D_d : d \in K\}$.**

$$\forall\, m \in M : D_d\,(E_e\,(m)) = m$$

System kryptograficzny nazywamy symetrycznym wtedy, gdy dla każdej pary kluczy (e, d) „obliczeniowo łatwe" jest określenie na podstawie znajomości jednego z kluczy z tej pary (np. klucza e) drugiego klucza (czyli klucza d).

W przypadku większości rozwiązań algorytmów i mechanizmów kryptografii symetrycznej e = d.

Szyfrowanie kluczem symetrycznym

Jeżeli odtworzenie jednego klucza na podstawie znajomości drugiego bez dodatkowej wiedzy („trapdoor”) jest „obliczeniowo trudne”, to taki system kryptograficzny zwany jest asymetrycznym (z reguły utożsamianym z tzw. „kryptografią klucza publicznego”).

Niekiedy wyróżnia się „kryptografię bezkluczową” i kwalifikuje do niej algorytmy kryptograficzne nie wymagające stosowania sekretów, np. funkcje skrótu wykorzystywane do ochrony integralności danych.

Składnia szyfrowania

Bardziej formalnie

Schemat szyfrowania kluczem prywatnym(symetrycznym) jest zdefiniowany poprzez określenie:

- Zbioru wiadomości *M* (a message space) – zbiór dozwolonych wiadomości
- 3 algorytmów:
  1. **Gen** – algorytm generowania klucza – algorytm probabilistyczny zwracający klucz *k* wybrany wg pewnego rozkładu
  2. **Enc** – algorytm szyfrowania – wejście: *k*, *m*, wyjście: szyfrogram: *c* ($\mathrm{Enc}_k(m)$)
  3. **Dec** – algorytm deszyfrowania – wejście: k, c, wyście m ($\mathrm{Dec}_k(c)$)

Czy algorytm szyfrujący powinien być tajny ?

„Security through obscurity ???"

August Kerckoffs (1835- 1903)

Kerckoff's principle (1883)

"Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.

„It (i.e. the cipher) should not require secrecy, and it should not be a problem if it falls into enemy hands"

Shannon's maxim (1948)

„one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them"

Bezpieczeństwo szyfru musi zależeć całkowicie od (bezpieczeństwa) klucza krypto-graficznego" (i to jest główne wymaganie w stosunku do algorytmu szyfrującego) !!!!

Podstawowe pojęcia - powtórka

- Tryby szyfrowanie, szyfrowanie plików, padding
- Szyfry asymetryczny
- Funkcja skrótu
- Podpis cyfrowy

Plan wykładu

1. Informacje o kursie
2. Podstawowe informacje o kryptologii
3. Zasady nowoczesnej kryptografii
4. Teoria informacji a kryptologia

Zasady nowoczesnej kryptografii

1. Formalne definicje

Jeśli nie rozumiesz, co chcesz osiągnąć, jak możesz się dowiedzieć, kiedy (lub jeśli) to osiągnąłeś?

- Jasne przedstawienie, przy jakich zagrożeniach, jakie mamy gwarancje bezpieczeństwa
- Modularność i możliwość wymiany komponentów
  - Nie należy zakładać, że definicje są trywialne i wszyscy je tak samo rozumieją
  - Definicja ma dwa składniki
    - Gwarancje bezpieczeństwa lub co oznacza udany atak
    - Model zagrożeń
- Przykład – szyfrowanie
  - Czy schemat w którym powiemy tylko, że jeżeli niemożliwe jest odtworzenie klucza to on będzie bezpieczny, jest poprawny?
  - Czy jeżeli nie będziemy mogli odtworzyć **całego** tekstu jawnego z szyfrogramu to schemat będzie bezpieczny?

Zasady nowoczesnej kryptografii

- **Nieformalnie**: Właściwa odpowiedź: niezależnie od jakichkolwiek informacji które atakujący już posiada, zaszyfrowany tekst nie powinien ujawniać żadnych dodatkowych informacji na temat tekstu jawnego („*security goal*”)
- Zakładamy możliwości atakującego, ale nie to jak je wykorzysta („*threat model*”):
  - Ciphertext-only attack
  - Known-plaintext attack
  - Chosen-plaintext attack
  - Chosen-ciphertext attack

2. Założenia – wprost i precyzyjne matematycznie
3. Dowody bezpieczeństwa

Plan wykładu

1. Informacje o kursie
2. Podstawowe informacje o kryptologii
3. Zasady nowoczesnej kryptografii
4. Teoria informacji a kryptologia

TEORIA INFORMACJI A KRYPTOLOGIA

Niech X będzie zmienną losową przybierającą wartości ze skończonego zbioru $\{x_1, x_2, ..., x_n\}$, przy czym rozkład prawdopodobieństwa tej zmiennej określony będzie przez zbiór wartości:

$$p_i = P(X = x_i) \qquad (i = 1, 2, ..., n)$$

a ponadto:

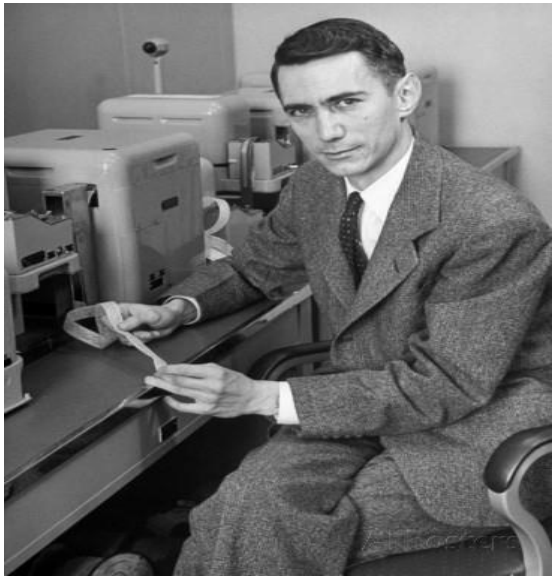
$$\sum_{i=1}^{n} p_i = 1$$

Rozkład ten, o ile nie będzie to wiodło do nieporozumień, będzie oznaczany jako p(X).

Entropia jest miarą ilości informacji pozyskanej w wyniku obserwacji zmiennej losowej X:

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i \quad \text{(w bitach)}$$

TEORIA INFORMACJI A KRYPTOLOGIA - GENEZA



1948

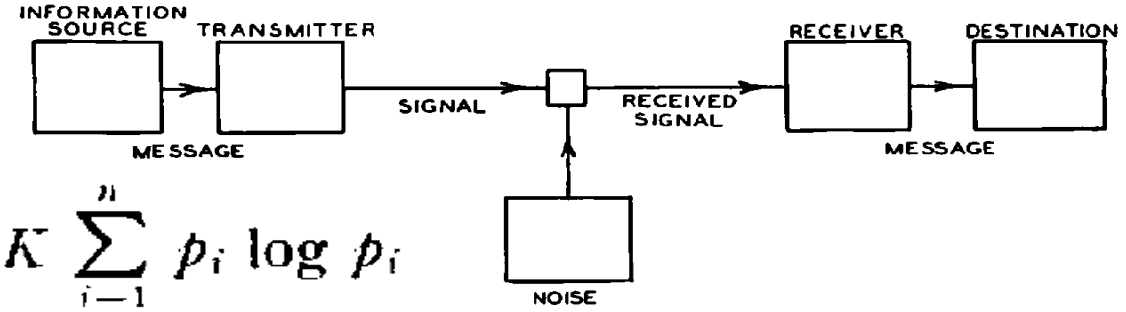
The Bell System Technical Journal

Vol. XXVII *July, 1948* *No. 3*

A Mathematical Theory of Communication

By C. E. SHANNON

Pojęcie entropii, jako miary ilości informacji i bitu jako jednostki informacji

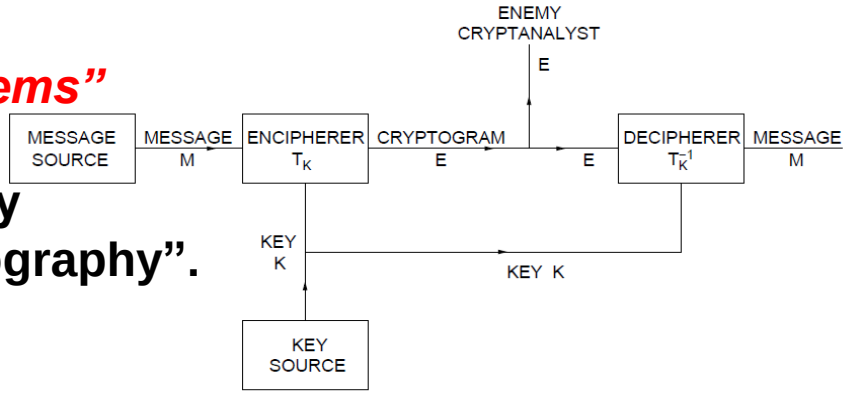


$$H = -K \sum_{i=1}^{n} p_i \log p_i$$

1949

„Communication theory of secrecy systems”

Praca ta została po raz pierwszy przedstawiona 1 września 1945 jako tajny raport „A Mathematical Theory of Cryptography”.



Z punktu widzenia kryptologii entropia wiadomości mierzy jej nieokreśloność, podając liczbę bitów informacji, jaka musi być pozyskana w celu jej ujawnienia, jeżeli wiadomość ta została ukryta w postaci zaszyfrowanej.

Każda dodatkowo pozyskana informacja zmniejsza entropię.

Właściwości entropii:

Dla zmiennej losowej mogącej przybierać n różnych wartości

$$0 \leq H(X) \leq \log_2 n$$

$$H(X) = 0 \Leftrightarrow p_i = 1 \text{ dla pewnego } i \text{ oraz } p_j = 0 \text{ dla wszystkich } j \neq i$$

$$H(X) = \log_2 n \Leftrightarrow p_i = 1/n \text{ dla każdego } i$$

Entropia łączna X i Y :

$$H(X, Y) = -\sum_{x,y} P(X = x, Y = y) \log_2 (P(X = x, Y = y))$$

$$H(X, Y) \leq H(X) + H(Y)$$

$$H(X, Y) = H(X) + H(Y) \Leftrightarrow X \text{ i } Y \text{ są niezależne}$$

Entropia warunkowa X dla Y = y:

$$H(X \mid Y = y) = -\sum_{x} P(X = x \mid Y = y) \log_2 (P(X = x \mid Y = y))$$

Entropia warunkowa X względem Y (*equivocation*):

$$H_Y(X) = H(X \mid Y) = -\sum_{y} P(Y = y) H(X \mid Y = y)$$

Wartość $H_Y(X)$ jest miarą nieokreśloności X po pozyskaniu obserwacji Y.

Wartość $H_Y(X)$ jest miarą nieokreśloności X po pozyskaniu obserwacji Y.

$$H_Y(X) \geq 0 \text{ oraz } H_X(X) = 0$$

$$H(X, Y) = H(X) + H_X(Y) = H(Y) + H_Y(X)$$

$$H_Y(X) \leq H(X)$$

$$H_Y(X) = H(X) \Leftrightarrow X \text{ i } Y \text{ są niezależne}$$

Informacja wzajemna (*transinformation*) zmiennych losowych X i Y:

$$I(X ; Y) = H(X) - H_Y(X)$$

jest interpretowana jako ilość informacji o X ujawniana na podstawie znajomości Y.

Niech będą dane:

$\mathcal{M}$ **- przestrzeń wiadomości jawnych M z rozkładem prawdopodobieństwa a priori p (M)**

$\mathcal{C}$ **- przestrzeń wiadomości zaszyfrowanych C z rozkładem prawdopodobieństwa p (C)**

$\mathcal{K}$ **- przestrzeń kluczy K wybieranych zgodnie z rozkładem prawdopodobieństwa p (K)**

Warunek poufności doskonałej : $p_C (M) = p (M)$

Interpretacja : przechwycenie zaszyfrowanej wiadomości nie daje żadnych przesłanek do określenia wiadomości jawnej.

Prawdopodobieństwo odbioru wiadomości zaszyfrowanej C pod warunkiem wysłania wiadomości jawnej M :

$$p_M(C) = \sum_{E_K(M)=C} p(K)$$

Warunek konieczny i wystarczający poufności doskonałej :

$$\forall\, C \in \mathscr{C}\ \forall\, M \in \mathscr{M} : p_M(C) = p(C)$$

Interpretacja : prawdopodobieństwo odebrania określonego kryptogramu C przy założeniu, że wysłano wiadomość M zaszyfrowaną pewnym kluczem, jest takie samo, jak prawdopodobieństwo odebrania C przy wysłaniu jakiejkolwiek innej wiadomości M' zaszyfrowanej dowolnym innym kluczem.

Wniosek:
Poufność doskonała wymaga, aby liczba kluczy była równa co najmniej liczbie wiadomości.

Niech dla ustalonego "języka" przestrzeń wiadomości jawnych zawiera komunikaty o długości N znaków, przy czym do ich przedstawienia wykorzystywany jest alfabet zawierający L znaków.

Wskaźnik języka (*rate of the language*) to ilość informacji (entropia) przypadająca na jeden znak wiadomości jawnej :

$$r = H(M)/N$$

Bezwzględny wskaźnik języka (*absolute rate of the language*) to maksymalna liczba bitów informacji, która mogłaby być zakodowana w jednym znaku, przy założeniu, że wszystkie możliwe sekwencje znaków są jednakowo prawdopodobne (maksymalna entropia dla pojedynczego znaku) :

$$R = \log_2 L$$

Nadmiarowość (*redundancy*) języka określana jest jako :

$$D = R - r$$

(czasem wyrażana także w procentach jako $100\ D\ /\ R$).

Przykład A:

Metodą szacowania entropii N-gramów dla rosnących wartości N określono dla literackiego języka angielskiego (26 liter) metodą ekstrapolacji (wykorzystując reprezentatywne wieloznakowe próbki tekstów) wartość wskaźnika języka jako :

$1.0 \leq r \leq 1.5$ bitów na literę

$R = \log_2 26 \approx 4.7$ bitów na literę

Nadmiarowość :

$3.2 \leq D \leq 3.7$ (68 % - 79 %)

Przykład B:

Wiadomości jawne są ciągami cyfr 0 - 9, zaś histogramy poszczególnych cyfr, digramów, trigramów, itd., są zbiorami identycznych wartości.

Entropia dla ciągów N-elementowych :

$H(M) = 10^N (1/10^N) \log_2(10^N) = \log_2(10^N) = N \log_2 10$

$r = \log_2 10 \approx 3.32$ bitów na cyfrę

$R = \log_2 10 \approx 3.32$ bitów na cyfrę

Nadmiarowość :

$D = 0$ (0 %)

Jeśli $p_C(K)$ jest prawdopodobieństwem warunkowym, że użyto klucza K, pod warunkiem, że przechwycono wiadomość tajną C, to poufność klucza można wyrazić przez entropię warunkową klucza (Shannon) :

$$H_C(K) = \sum_{C} p(C) \sum_{K} p_C(K) \log_2(1 / p_C(K))$$

Jeżeli $H_C(K) = 0$, to brak nieokreśloności i szyfr jest teoretycznie przełamywalny, pod warunkiem zgromadzenia wystarczających do tego celu zasobów.

Ze wzrostem długości N tekstu zaszyfrowanego zmniejsza się entropia warunkowa klucza.

Długość krytyczna (*unicity distance*) jest to najmniejsza wartość N, dla której $H_C(K) = 0$, a więc najmniejsza ilość zaszyfrowanego tekstu niezbędna do jednoznacznego określenia klucza szyfrowania K (dla szyfru bezwarunkowo bezpiecznego $H_C(K)$ nigdy nie osiąga wartości zerowej, takim szyfrem jest np. „one-time pad" Vernama z 1917 roku, w którym długość klucza szyfrującego jest równa długości tekstu jawnego).

W większości przypadków nie jest możliwe analityczne wyznaczenie wartości długości krytycznej. Niekiedy można ją jednak oszacować. Np. dla szyfru endomorficznego, w którym wszystkie wiadomości jawne i tajne mają długość N i są wyrażane symbolami tego samego alfabetu, zawierającego L znaków, Hellman oszacował długość krytyczną szyfru jako $N = H(K) / D$.

Przykład C:

Szyfrem podstawieniowym Cezara zaszyfrowano tekst angielski, składający się jedynie z dużych liter (alfabet przestrzeni wiadomości jawnych i tajnych zawiera 26 znaków). Kluczem szyfrowania jest wielkość przesunięcia (od 0 do 25).

Nadmiarowość języka angielskiego : $D = 3.2$

Entropia przestrzeni kluczy : $H(K) = \log_2 26 = 4.7$

Długość krytyczna : $N = (4.7) / (3.2) \approx 1.5$ znaku (PARADOKS ???!!!)

Przykład D:

Dla systemu kryptograficznego z przykładu B nadmiarowość wynosi $D = 0$, a zatem teoretycznie nie jest możliwe określenie liczby znaków niezbędnych do jednoznacznego określenia klucza.

Przykład E („ciekawostka przyrodnicza” i inspiracja do refleksji):
Blokowy algorytm kryptografii symetrycznej DES szyfruje bloki 64-bitowe do 64-bitowych kryptogramów za pomocą 56-bitowego klucza.

Można go „od biedy” potraktować jako szyfr endomorficzny, w którym alfabet wiadomości jawnych i alfabet kryptogramów liczą 2^{64} różnych symboli (pojedynczym symbolem jest każdy 64-bitowy ciąg).

Przestrzeń kluczy liczy 2^{56} elementów, a zatem oczekiwana złożoność ataku brutalnego to 2^{55} prób. Kryptoanaliza liniowa DES (Matsui) wymaga 2^{47} prób.

Gdyby założyć, że tekst jawny w języku angielskim jest kodowany w ASCII i zawiera tylko duże litery bez spacji, zaś każdy 8-bajtowy/8-znakowy ciąg zachowuje nadmiarowość języka, to wówczas:

Nadmiarowość języka angielskiego : $D = 3.2$
Entropia przestrzeni kluczy : $H(K) = \log_2(2^{56}) = 56$
Długość krytyczna : $N = 56 / 3.2 \approx 17.5$ **znaku**

Tak, ale alfabetu, którego znakami są wszystkie ciągi 64-bitowe, a poza tym już 19 stycznia 1999 distributed.net oraz RSA Labs złamały szyfr w niecałe 24 godziny za pomocą ataku brutalnego.

Koniec części 1