CURS 5
PRINCIPIILE CRIPTOGRAFIEI MODERNE

- **Auguste Kerckhoffs** – ***La Cryptographie Militaire*** **(1883)**

  1. **Principiul lui Kerckhoffs:** Sistemul nu trebuie să fie secret, deoarece poate să cadă oricând în mâinile inamicului (i.e., securitatea unui sistem de criptare constă doar în menținerea secretă a cheii).

- **Claude Shannon** – ***A Mathematical Theory of Cryptography*** **(1945)**

  1. **Reformularea principiului lui Kerckhoffs**: "The enemy knows the system!"

  2. **CONFUZIE**: orice caracter din textul cifrat depinde de cât mai multe caractere din cheia secretă pentru a ascunde corelațiile dintre ele

  3. **DIFUZIE:** structura statistică a mesajului clar trebuie să fie ascunsă/disipată în mesajul criptat (http://practicalcryptography.com/cryptanalysis/letter-frequencies-various-languages/english-letter-frequencies/)

  4. **CRITERIUL STRICT DE AVALANȘĂ** (echivalent cu difuzia): modificarea unui singur caracter din mesajul clar trebuie să ducă la modificare a cel puțin jumătate dintre caracterele mesajului criptat

- Rolul confuziei și difuziei este acela de a împiedica criptanaliza bazată pe statistică!
- Confuzia se asigură prin operații de substituție cu funcții neliniare, dar, totuși rămân anumite șabloane în textul criptat.
- Difuzia are rolul de elimina/minimiza șabloanele rămase în mesajul criptat, folosind operații de fracționare și permutare.

Mesaj clar: EXEMPLU
Substituție: YTTXAMA
Fracționare:
01011001010101000101010001011000010000010100110101000001
Permutare:
00110001001011000100011100100110100101101001000001000101
Mesaj criptat: 1,G&û à

- În lucrare sa *Communication Theory of Secrecy Systems* din 1949 Claude Shannon a afirmat faptul că un cifru foarte bun (i.e., rezistent la atacuri criptografice) se obține aplicând mai multe runde de confuzie și difuzie (*cifrul compus*)!!!

SECURITATEA PERFECTĂ

Tipuri de securitate a unui cifru:

1. *securitate necondiționată*: cifrul nu poate fi spart chiar dacă atacatorul are la dispoziție resurse computaționale infinite;
2. *securitate computațională*: cel mai bun algoritm cunoscut de spargere a cifrului are o complexitate minimă foarte mare (de exemplu, complexitate exponențială);
3. *securitate demonstrabilă*: securitatea cifrului este echivalentă cu rezolvarea unei probleme greu-rezolvabile (Clasele de complexitate P și NP - Wikipedia);
4. *securitate euristică*: nu se cunoaște niciun algoritm de spargere a cifrului.

Tipuri de atacuri criptografice:

1. *atacul cu text cifrat* (*Ciphertext Only Attack*): criptanalistul are la dispoziție doar mesaje cifrate, respectiv nu are nicio informație despre mesajele clare din care acestea provin;
2. *atacul cu text clar cunoscut* (*Known Plaintext Attack*): criptanalistul are la dispoziție mesaje cifrate și porțiuni din mesajele clare corespunzătoare lor;
3. *atacul cu text clar ales* (*Chosen Plaintext Attack*): criptanalistul are la dispoziție mesajele cifrate corespunzătoare unor mesajele clare alese de el;
4. *atacul cu forță brută* (*Brute Force Attack*): criptanalistul încearcă să determine cheia secretă utilizată testând toate posibilele chei secrete;
5. *atacuri pe canale colaterale* (*Side-channel Attacks*): sunt atacuri care utilizează orice informație provenită, în mod neintenționat, din dispozitivele electronice care implementează primitive criptografice: durată de procesare, sunet, unde electromagnetice, putere disipată etc. (Side-channel attack - Wikipedia)

Mai multe informații despre tipurile de atacuri criptografice găsiți în pagina următoare: Attacks On Cryptosystems - Tutorialspoint!

Securitate perfectă (Shannon – 1949): Textul criptat nu trebuie să furnizeze nicio informație despre textul clar!

Formulare echivalentă:
Pentru orice mesaj criptat C și oricare două mesaje clare $P_1 \neq P_2$, avem:

$$\text{Prob}[enc_K(P_1) = C] = \text{Prob}[enc_K(P_2) = C]$$

Exemplu: Cifrul lui Cezar NU are securitate perfectă decât pentru mesaje de lungime 1!

$$\underbrace{\text{Prob}[enc_K(\text{"}AB\text{"}) = \text{"}BC\text{"}]}_{\frac{1}{26}\text{ (pentru cheia } K=1\text{)}} \neq \underbrace{\text{Prob}[enc_K(\text{"}BP\text{"}) = \text{"}BC\text{"}]}_{0}$$

Teoremă (Shannon): În orice cifru cu securitate perfectă trebuie ca lungimea cheii secrete să fie cel puțin egală cu lungimea mesajului clar.

Exemplu: Cifrul lui Cezar în care schimbăm cheia secretă pentru fiecare literă din mesajul clar are securitate perfectă!

Teoremă (Shannon): Considerăm un cifru în care numărul mesajelor clare, numărul mesajelor criptate și numărul cheilor secrete sunt egale toate cu n. Atunci cifrul respectiv are securitate perfectă dacă și numai dacă:

1. orice cheie secretă este folosită cu probabilitatea $\frac{1}{n}$;
2. pentru orice mesaj clar P și orice mesaj criptat C există și este unică o cheie secretă K astfel încât $enc_K(P) = C$.

Cifrul One-time Pad (OTP)

Cifrul OTP a fost inventat de către Frank Miller în anul 1882.

Criptarea se realizează folosind o cheie secretă aleatorie de aceeași lungime cu mesajul clar și adunând modulo 26 codurile literelor aflate pe aceeași poziție (codul unei litere este dat de poziția sa în alfabetul limbii engleze, începând de la poziția 0 pentru litera A). Decriptarea se realizează folosind aceeași cheie secretă și scăzând modulo 26 codurile literelor aflate pe aceeași poziție.

Exemplu:

Codurile literelor din alfabetul englez:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Criptare:

Mesaj clar	A	T	A	C	A	M	L	A	N	O	R	D
	0	19	0	2	0	12	11	0	13	14	17	3
Cheie secretă	B	X	T	C	B	A	A	V	D	G	K	M
	1	23	19	2	1	0	0	21	3	6	10	12
Mesaj criptat	B	Q	T	E	B	M	L	V	Q	U	B	P
	1	16	19	4	1	12	11	21	16	20	1	15

Decriptare:

Mesaj criptat	B	Q	T	E	B	M	L	V	Q	U	B	P
	1	16	19	4	1	12	11	21	16	20	1	15
Cheie secretă	B	X	T	C	B	A	A	V	D	G	K	M
	1	23	19	2	1	0	0	21	3	6	10	12
Mesaj decriptat	A	T	A	C	A	M	L	A	N	O	R	D
	0	19	0	2	0	12	11	0	13	14	17	3

(16-23) modulo 26 = (-7) modulo 26 = (26-7) modulo 26 = 19 modulo 26 = 19

Teoremă (Shannon): Cifrul OTP are securitate perfectă.

Demonstrația teoremei se bazează pe faptul că orice mesaj criptat poate să provină din orice mesaj clar folosind o unică cheie secretă și invers! Astfel, dacă decriptăm un mesaj criptat de lungime n folosind toate cheile secrete posibile de lungime n vom obține toate mesajele clare posibile de lungime n, deci nu putem decide din ce mesaj clar provine textul criptat!

De exemplu, pentru mesajul criptat anterior se poate determina ușor cheia secretă pentru care mesajul respectiv se va decripta în **ATACAMLAVEST**:

Mesaj criptat	B	Q	T	E	B	M	L	V	Q	U	B	P
	1	16	19	4	1	12	11	21	16	20	1	15
Cheie secretă	B	X	T	C	B	A	A	V	V	Q	J	W
	1	23	19	2	1	0	0	21	21	16	9	22
Mesaj decriptat	A	T	A	C	A	M	L	A	V	E	S	T
	0	19	0	2	0	12	11	0	21	4	18	19