CURS 6
SECURITATEA PERFECTĂ

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:

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

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

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 Vernam

Cifrul Vernam a fost inventat de către Gilbert Vernam în anul 1917.

Criptarea se realizează considerând mesaje binare și folosind o cheie secretă binară aleatorie de aceeași lungime cu mesajul clar și adunând modulo 2 biții aflați pe aceeași poziție (operația XOR / sau-exclusiv). Decriptarea se realizează simetric, folosind aceeași cheie secretă și operația XOR.

^ = sau-exclusiv/XOR

^	0	1
0	0	1
1	1	0

```
x = 133 = 00010000101
y = 2020 = 11111100100
x ^ y = 1889 = 11101100001
```

a ^ b = 1 <=> a ≠ b

Proprietățile operatorului XOR (adunare modulo 2 = $\oplus$):

a) `t ^ t = 0`
b) `t ^ 0 = t`
c) `t ^ v = v ^ t`
d) `(t ^ v) ^ w  = t ^ (v ^ w)`

Cifrul Vernam (1917):

Se consideră un mesaj binar clar P și o cheie fluidă K (cu aceeași lungime ca mesajul clar P) comună.

Mesajul criptat C se obține astfel:

$$C_i = P_i \oplus K_i$$

Mesajul decriptat P se obține astfel:

$$P_i = C_i \oplus K_i$$

Criptare	Decriptare	Determinarea cheii secrete
P = 00010000101 K = 11111100100 ⊕ --------------- C = 11101100001	C = 11101100001 K = 11111100100 ⊕ --------------- P = 00010000101	C = 11101100001 P = 00010000101⊕ --------------- K = 11111100100

Corectitudinea decriptării: $P_i = C_i \oplus K_i = \underbrace{P_i \oplus K_i}_{C_i} \oplus K_i = P_i \oplus 0 = P_i$

Determinarea cheii secrete: $P_i = C_i \oplus K_i \Rightarrow P_i \oplus C_i = C_i \oplus K_i \oplus C_i \Rightarrow K_i = C_i \oplus P_i$

Pericolul utilizării aceleași chei fluide pentru două mesaje diferite:

$C_1 = P_1 \oplus K_1$
$C_2 = P_2 \oplus K_1$

$C_1 \oplus C_2 = P_1 \oplus K_1 \oplus P_2 \oplus K_1 = P_1 \oplus P_2$

Folosind proprietățile statistice ale textelor clare se pot deduce proprietăți statistice ale textelor criptate și corelații dintre ele! Un exemplu celebru în acest sens este proiectul Venona: https://en.wikipedia.org/wiki/Venona_project!

Limitări ale utilizării în practică a cifrurilor OTP/Vernam:

1. Generarea și stocarea tuturor posibilelor chei secrete (fluide) depășesc cu mult stadiul actual al tehnologiei IT:

   - **OTP:** cheile secrete formate din 100 de litere sunt în număr de 26^{100}, adică ar necesita aproximativ $4.7*10^{139}$ de pagini scrise cu un font de dimensiune 8 (aproximativ 66 de chei secrete pe o pagina)!
   - **Vernam:** cheile secrete formate din 1024 de biți (adică 128 de caractere!!!) sunt în număr de 2^{1024}, adică ar necesita un spațiu de stocare de aproximativ 2^{1024} biți = 2^{1021} octeți = 2^{1011} KB = 2^{1001} MB = 2^{991} GB = 2^{981} TB = 2^{971} PB (petabytes) = 2^{961} EB (exabytes) = 2^{951} ZB (zettabytes)!

     Spațiul necesar de stocare (2^{951} ZB):
     1903381642851562320381519997631872716968013058124024907591
     3879799244040411653175981378154425550801287549423664514470
     0550458186911429747930597226314381106512100220267577274863
     8646638604587901103193906170601409839623766718344803686512
     84108664364628234625541773498130420841441964648279572 48 **ZB**

     Spațiul total de stocare la nivel mondial estimat pentru anul 2025 (The Digitization of the World from Edge to Core (seagate.com)): 175 **ZB**

   - **Timpul necesar generării tuturor cheilor secrete formate din 1024 de biți este de ordinul miliardelor de miliarde de ani!!!**

2. Schimbul greoi de chei secretă: o cheie secretă trebuie să aibă aceeași lungime cu mesajul clar și poate fi utilizată o singură dată!!!

CIFRURI FLUIDE

Cifru fluid = un cifru de tip Vernam în care se utilizează o cheie fluidă de aceeași lungime cu mesajul clar, generată folosind un generator de numere pseudo-aleatorii (PRNG = PseudoRandom Numbers Generator).

Un cifru fluid poate fi:
- *sincron* – cheia fluidă este independentă de mesajul clar și de cel criptat;
- *asincron* – cheia fluidă depinde de un număr fixat de biți anterior criptați.

Un **generator de numere pseudo-aleatorii** este un algoritm care este aplicat în mod iterativ asupra unor valori inițiale pentru a obține un șir de valori pseudo-aleatorii.

Valorile inițiale ale generatorului (inclusiv parametrii săi) vor forma cheia secretă a unui cifru fluid, iar valorile generate vor forma cheia fluidă!!!

Generatorul liniar congruențial (LCG)

$$x_{n+1} = (3x_n + 7) \bmod 11$$

$x_0 = 3$ (valoare inițială = seed)

$x_1 = (3x_0 + 7) \bmod 11 = (3 * 3 + 7) \bmod 11 = 16 \bmod 11 = 5$

$x_2 = (3x_1 + 7) \bmod 11 = (3 * 5 + 7) \bmod 11 = 22 \bmod 11 = 0$

$x_3 = (3x_2 + 7) \bmod 11 = (3 * 0 + 7) \bmod 11 = 7 \bmod 11 = 7$

$x_4 = (3x_3 + 7) \bmod 11 = (3 * 7 + 7) \bmod 11 = 28 \bmod 11 = 6$

$x_5 = (3x_4 + 7) \bmod 11 = (3 * 6 + 7) \bmod 11 = 25 \bmod 11 = 3$

$x_6 = (3x_5 + 7) \bmod 11 = (3 * 3 + 7) \bmod 11 = 16 \bmod 11 = 5$

$x_7 = (3x_6 + 7) \bmod 11 = (3 * 5 + 7) \bmod 11 = 22 \bmod 11 = 0$

De exemplu, pentru generatorul de mai sus cheia secretă va fi formată din $a = 3, b = 7,\ m = 11$ și $x_0 = 3$, iar cheia fluidă pe care o vor folosi într-un cifru Vernam este formată din numerele generate de LCG: 3, 5, 0, 7, 6, 3 ,5, 0, 7, 6, ...