

AES, RC4, RSA



AES, RC4, RSA

Văduva Vlad-Andrei

RC4

Compus din 2 părți: KSA și PRGA

KSA: $+$

- Creăm un array S de 256 de bytes
- Generăm diferite permutări ale array-ului S folosind formula $i = (i + \text{schedule}[j] + t[j]) \% 256$

PRGA:

- Output-ul de la KSA este trimis ca input pentru PRGA, care generează o cheie bazată pe array-ul S
- Va rezulta un keystream

Criptare:

Efectuăm operații XOR între fiecare caracter din plaintext si fiecare caracter din keystream.

○

RSA

- Generam două numere prime p și q
- Cheia publică este formată din n și e , unde $n=p*q$
- e se calculează astfel: $\frac{1}{\phi(n)}$ ●

$$\phi=(p-1)(q-1)$$

$$1<e<\phi, \gcd(e,\phi)=1$$

- Calculăm cheia privată cu formula $d = (k*\Phi(n) + 1) / e$, unde k este un număr întreg

Criptare:

Ex.: "HI": $H=8, I=9$

Rezultatul criptării va fi: $c=89^{e \bmod n}$

Pentru decriptare, folosim cheia privată: $c^{d \bmod n}$



AES

AES, RC4, RSA

- Criptarea presupune 4 pași: +
- SubBytes: Fiecare byte din bloc este înlocuit cu valoarea corespunzătoare din S-box
- ShiftRows: Fiecare rând din bloc este shiftat la stânga. Primul rând nu este shiftat deloc, al doilea este shiftat cu un byte, al treilea cu doi bytes, iar al patrulea cu 3 bytes.
- MixColumns: Fiecare coloană din bloc este transformată folosind produsul matricelor.
- AddRoundKey: Se efectuează o operație XOR între fiecare byte din block și byte-ul corespunzător din round key. Round key-ul este generat folosind un key schedule creat utilizând cheia secretă.

MULTUMESC!

