ALGORITMI DE CRIPTARE

Diana Anton


RSA
(RIVEST-SHAMIR-ADLEMAN)

METODĂ

Algoritm asimetric cu chei publice/private

- Se aleg două numere prime, ***p = 3 și q = 5***
- Se generează modulul RSA: ***num = p * q***
- Se calculează ***phi = (p - 1) * (q - 1)***
- Se alege exponentul cheiei publice ***1 < encrypt < phi,*** unde encrypt și phi sunt prime între ele.
- Se calculează exponentul cheiei private ***decrypt = (1 + (constant * phi)) / encrypt***

Cheie publică = ***{encrypt, num}***
Cheie privată = ***{decrypt, num}***
Criptare: ***(msg ^ encrypt) % num = crypt***
Decriptare: ***(crypt ^ decrypt) % num***


CIFRUL LUI CAESAR

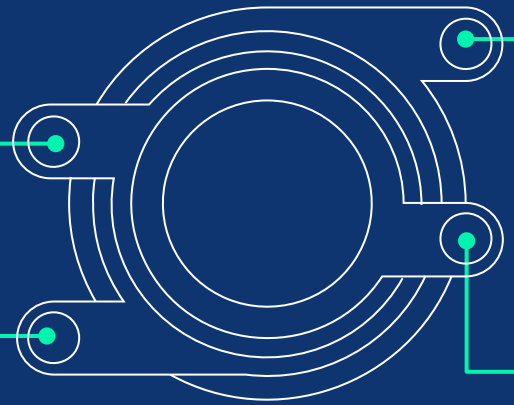
CUM FUNCȚIONEAZĂ

SCURT ISTORIC

Printre cele mai vechi cifruri existent, numit după Julius Caesar

CRIPTARE - CHEIE

Cheie -> număr între 1 și 25



CRIPTARE - METODĂ

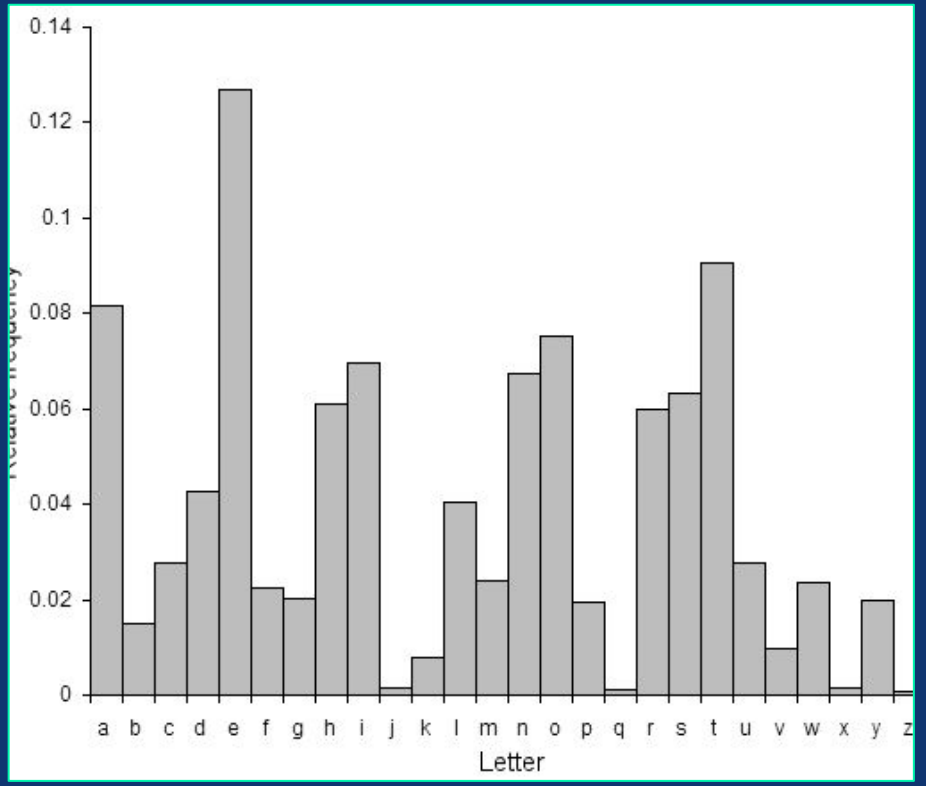
Fiecare literă din mesaj se mută cu x poziții în alfabet, x fiind cheia.

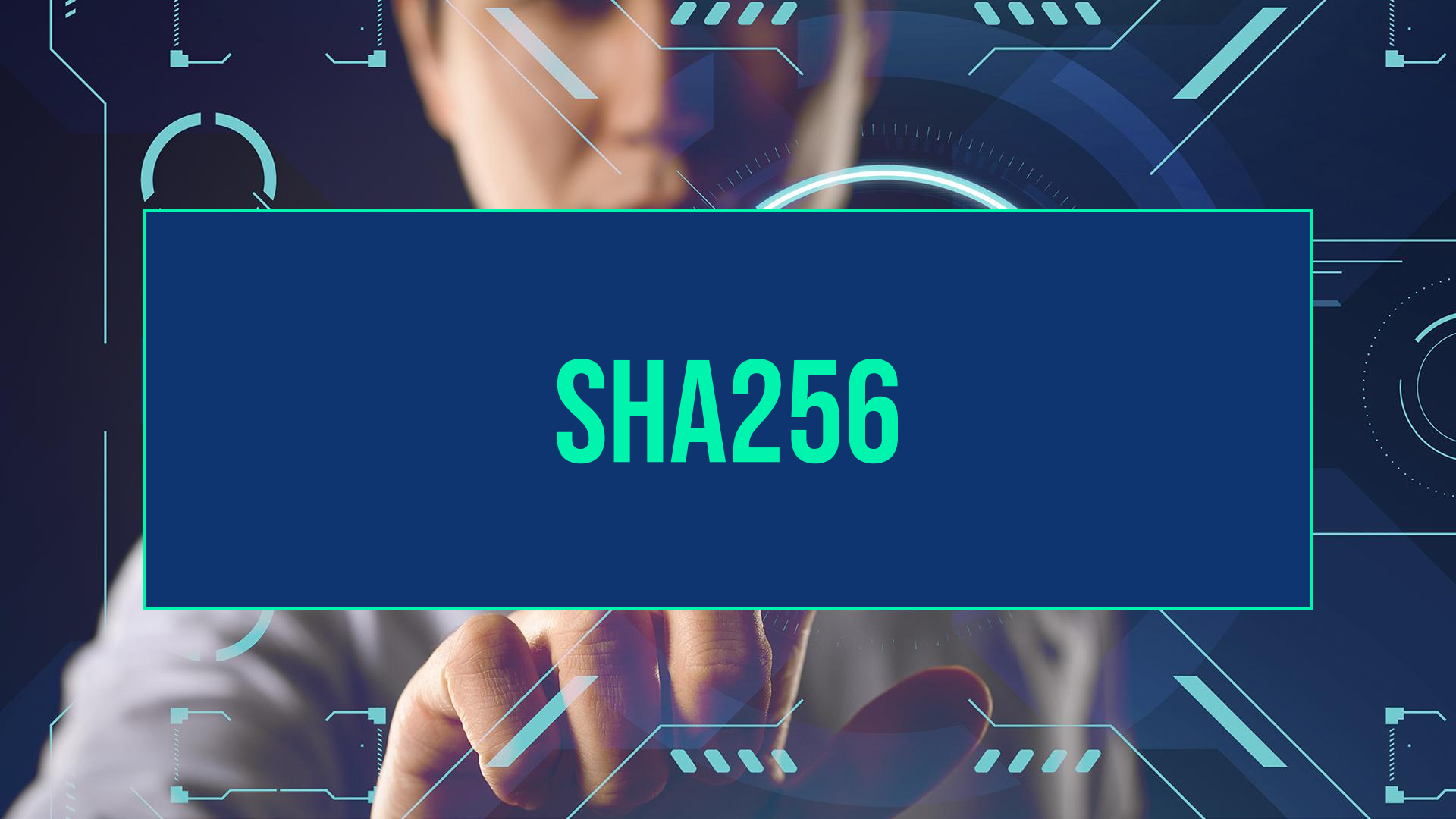
EXEMPLU

Cheie = 3
Mesaj = ABC
A -> D, B -> E, C -> F
Cod = DEF

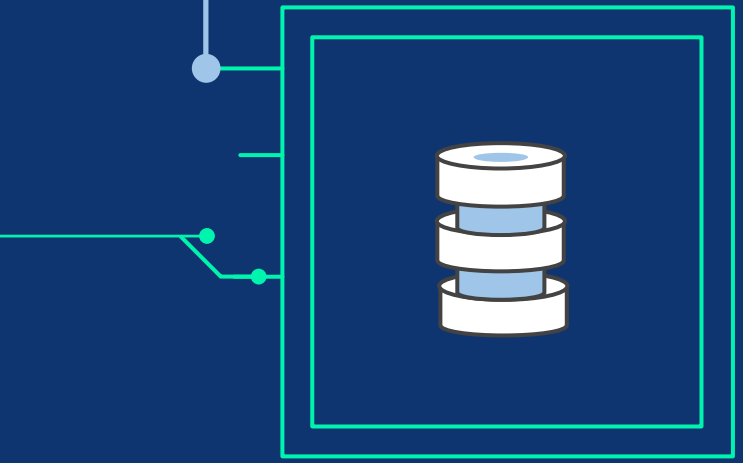
CRIPTANALIZA

- Brute Force asupra cifrului, fiind doar 26 de variante posibile
- Calcularea distribuției de frecvență a literelor din text




SHA256

EXEMPLU SIMPLU

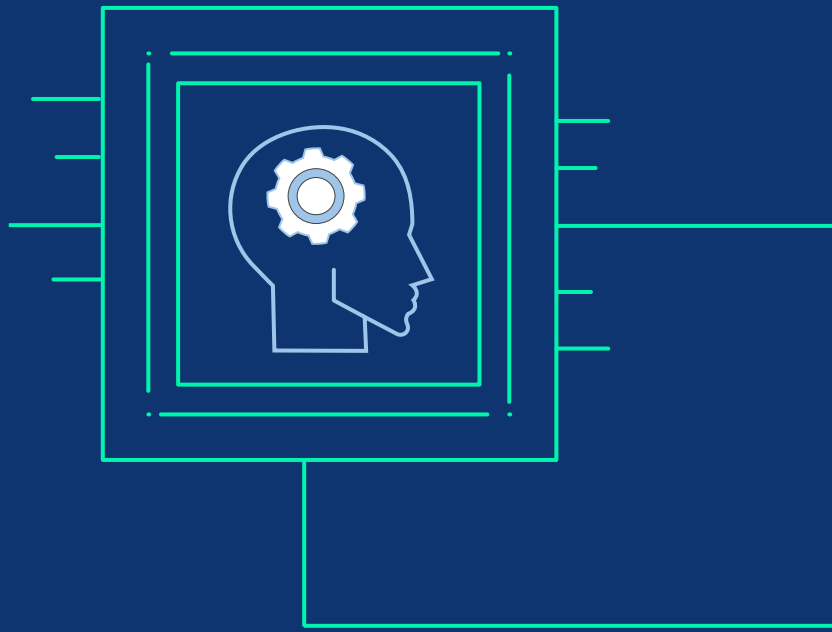


- Mesajul inițial: Hello
- Aleg numărul 123
- A = 1, B = 2 ….
- Spațiu = 27
- HELLO = 8 5 12 12 15
- Înmulțesc numărul ales cu valoarea primei litere. Dacă rezultatul e mai mare de 3 cifre, le aleg doar pe ultimele 3. Repet procedura cu rezultat * valoarea următoarei cifre.

123 * 8 = 984
984 * 5 = 4920
920 * 12 = 11040
104 * 12 = 1248
248 * 15 = 3720

PRE-PROCESARE

- Se convertește mesajul în binar
- Se adaugă la final 1
- Se umple cu 0 până valoare e un multiplu de 512 minus 64 biți
- Se adaugă 64 biți la final care reprezintă lungimea mesajului inițial
- Valoarea obținută va fi tot timpul divizibilă cu 512



THANKS!

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**

Please keep this slide for attribution