

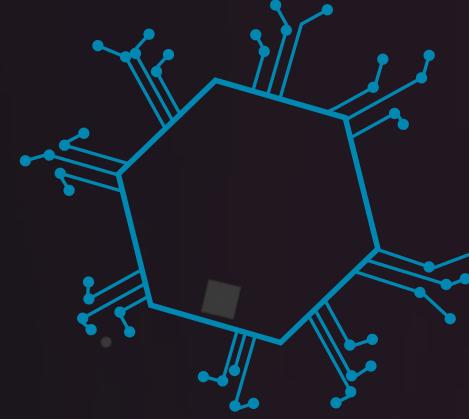
FMCC II - CRIPTOGRAFIA ELGAMAL

Guilherme Noronha

Pedro Leal

Pedro Nascimento

INTRODUÇÃO



1. Definição

- Sistema de criptografia assimétrica que usa um par de chaves: pública (para cifrar) e privada (para decifrar).

2. Base Matemática

- Fundamentado na Matemática Discreta: aritmética modular, teoria dos números, grupos cíclicos e corpos finitos.

3. Segurança

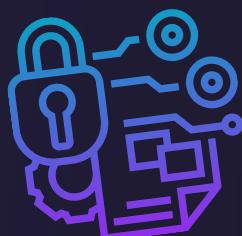
- Depende da dificuldade do problema do logaritmo discreto, considerado inviável de resolver com força bruta em chaves grandes.

4. Funcionamento

- Permite a criptografia por qualquer usuário com a chave pública, mas apenas o dono da chave privada pode descriptografar.

5. Aplicações

- Utilizado em assinaturas digitais, troca de chaves e sistemas de segurança de dados.





SEGURANÇA

A criptografia ElGamal é segura porque se baseia na dificuldade de resolver o problema do logaritmo discreto, considerado inviável para números primos grandes. Mesmo conhecendo a chave pública (valores p , r , a), descobrir a chave privada x é extremamente difícil. Além disso, ElGamal usa um valor aleatório diferente a cada encriptação, impedindo que a mesma mensagem gere o mesmo texto cifrado, o que protege contra ataques por padrões. Para decifrar uma mensagem interceptada, seria necessário resolver problemas matemáticos complexos (logaritmos discretos), algo impraticável com a tecnologia atual. A segurança depende do tamanho do primo p , da escolha dos parâmetros e da aleatoriedade.

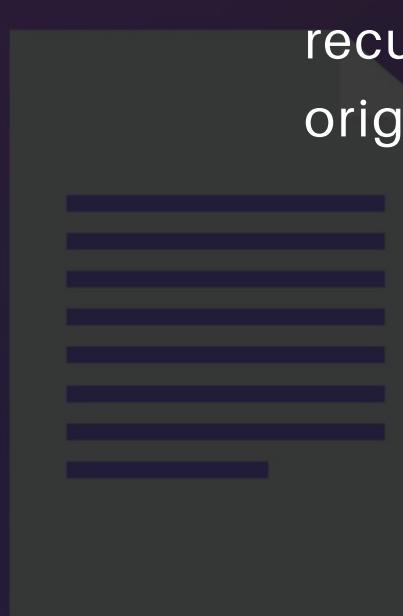




PASSOS DO SISTEMA CRIPTOGRÁFICO

0101
0101
0101

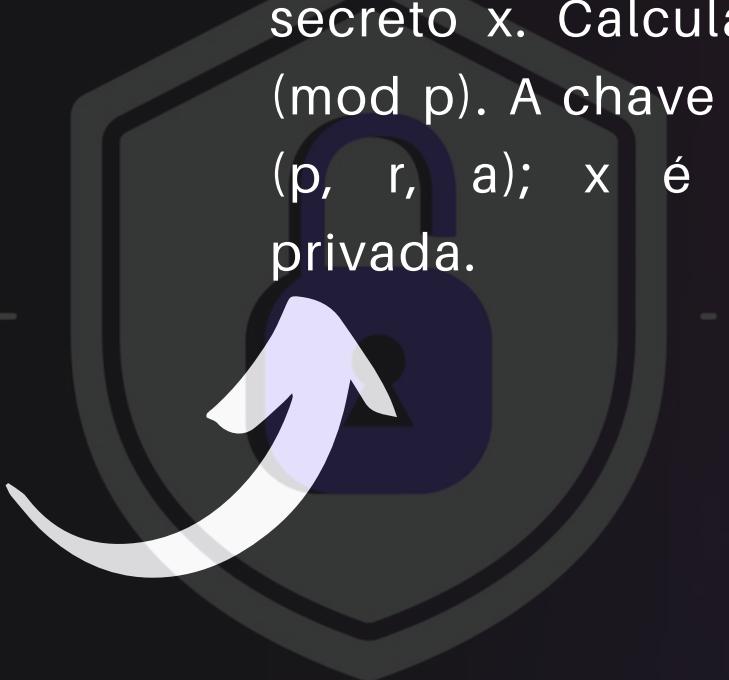
O receptor usa sua chave privada x para calcular $P = C \cdot b^{(p - 1 - x)} \pmod{p}$, recuperando o valor original da mensagem M .



O emissor escolhe um número aleatório y , calcula $b = r^y \pmod{p}$ e $C = M \cdot a^y$. O par cifrado (b, C) é enviado ao receptor.



O receptor escolhe um primo grande p , uma raiz primitiva r , e um número secreto x . Calcula $a = r^x \pmod{p}$. A chave pública é (p, r, a) ; x é a chave privada.



A mensagem é convertida para um número K (ou blocos M) menor que p , usando uma codificação acordada (ex: A = 00, B = 01...).

