

INTRODUÇÃO



RSA

ALGORITMOS DA CRIPTOGRAFIA
ASSIMÉTRICA.

CHAVE PÚBLICA

USADA PARA CRIPTOGRAFAR

CHAVE PRIVADA

USADA PARA DESCRIPTOGRAFAR



RSA **CONCEITO**



São usadas duas chaves diferentes e matematicamente relacionadas para garantir a segurança de informações digitais. Essas chaves formam um par, mas é praticamente impossível descobrir a chave privada conhecendo apenas a pública. Isso ocorre porque são utilizadas operações com números primos grandes e na aritmética modular. Seu princípio de segurança depende da dificuldade de fatorar um número muito grande em seus dois primos originais.

- Cifrar mensagens: o remetente usa a chave pública do destinatário para transformar o texto original em um número cifrado.
- Decifrar mensagens: apenas o destinatário, com sua chave privada, consegue reverter o processo.

PASSO A PASSO **FUNDAMENTO MATEMÁTICO**

1. ESCOLHA 2 NÚMEROS PRIMOS GRANDES DE TAMANHO SIMILAR QUE SERÃO REPRESENTADOS POR "P" E "Q".
2. CÁLCULO DO PRODUTO: UTILIZA-SE A EQUAÇÃO $N=P \times Q$, ONDE "N" SERÁ USADO COMO MÓDULO, OU SEJA, A PARTE DA CHAVE PÚBLICA E PRIVADA.
3. CÁLCULO DA FUNÇÃO TOTIENTE DE EULER: $\Phi(N) = (P-1) \times (Q-1)$ ESSA FUNÇÃO OBJETIVA CALCULAR O NÚMERO DE INTEIROS POSITIVOS MENORES QUE "N" QUE SÃO COPRIMOS, OU SEJA, QUE NÃO TENHA DIVISORES COMUNS, A "N", QUANDO "N" É O PRODUTO DE DOIS PRIMOS DISTINTOS "P" E "Q".
4. ESCOLHER O EXPOENTE PÚBLICO "E": $\text{GCD}(E, \Phi(N))$, "GCD" É O MÁXIMO DIVISOR COMUM, E ESSA FÓRMULA SERVE PARA CONTAR QUANTOS NÚMEROS MENORES QUE "N" SÃO COPRIMOS COM "N".
5. CÁLCULO DO EXPOENTE PRIVADO "D": $D \times E \equiv 1 \pmod{\Phi(N)}$, É UTILIZADO PARA ENCONTRAR O INVERSO MODULAR, QUE É EXATAMENTE O QUE "D" REPRESENTA EM RELAÇÃO A "E" E " $\Phi(N)$ " NA EQUAÇÃO.

EXEMPLO

ETAPA 1 – ESCOLHA DE DOIS NÚMEROS PRIMOS

$$p = 61$$

$$q = 53$$

ETAPA 2 – CÁLCULO DE N

O VALOR DE N SERÁ PARTE DA CHAVE PÚBLICA E DA CHAVE PRIVADA.

$$n = p \times q$$

$$n = 61 \times 53 = 3233$$

ETAPA 3 – TOTIENTE DE EULER ($\phi(n)$)

O TOTIENTE INDICA QUANTOS NÚMEROS SÃO COPRIMOS DE N.

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

$$\phi(n) = 60 \times 52 = 3120$$

ETAPA 4 – ESCOLHA DO EXPOENTE PÚBLICO (E)

PRECISAMOS DE UM NÚMERO $1 < E < \phi(n)$ QUE SEJA COPRIMO DE $\phi(n)$.

$$e = 17$$

ETAPA 5 – CÁLCULO DO EXPOENTE PRIVADO (D)

D É O INVERSO MULTIPLICATIVO DE E MÓDULO $\phi(n)$, OU SEJA:

$$d \times e \equiv 1 \pmod{\phi(n)}$$

$$d \times 17 \equiv 1 \pmod{3120}$$

$$d \times 17 = 1 + 3120 \times k$$

$$10 / 3$$

$$3 \times 3 = 9$$

SOBRA 1

$$10 = (3 \times 3) + 1$$

$$10 \equiv 1 \pmod{3}$$

$$10 = 1 + 3 \times K$$

$$K = 3$$

EXEMPLO

PARA K = 15, OBTEMOS:

$$(1 + 3120 \times 15) \div 17 = (1 + 46800) \div 17 =$$

$$46801 \div 17 = 2753$$

$$d = 2753$$

CHAVE PÚBLICA

$$E = 17, N = 3233$$

CHAVE PRIVADA

$$D = 2753, N = 3233$$

Tentando valores de k até achar um d inteiro:

k	$1 + 3120 \times k$	$(1 + 3120 \times k) \div 17$	d inteiro?
1	3121	183,588...	✗
2	6241	367,117...	✗
3	9361	550,647...	✗
4	12481	734,176...	✗
5	15601	917,705...	✗
6	18721	1101,235...	✗
7	21841	1284,764...	✗
8	24961	1468,294...	✗
9	28081	1651,823...	✗
10	31201	1835,352...	✗
11	34321	2018,882...	✗
12	37441	2202,411...	✗
13	40561	2385,941...	✗
14	43681	2569,470...	✗
15	46801	2753	✓