



CRIPTOGRAFIA

RSA conta:

$$n = p \times q$$

$$z = (p - 1)(q - 1)$$

e (criptografa dependendo do contexto) e $< n$;

e é coprimo de z, ou seja, não têm divisores comuns

$$d \rightarrow e \cdot d \bmod z = 1 \text{ (resto da divisão tem que ser 1)}$$

chave pública = (n, e)

chave privada = (n, d)

EXPLICAÇÃO → Criptografia Assimétrica → Tamanho da chave (512 - 4094 bits)

(RSA) → Algoritmos + difíceis → Usa o produto de 2 primos grandes com 100-200 dígitos. Browsers utilizam.

Criptosistema (Confidencialidade)

- Remetente usa a pública do destinatário e criptografa.
- Destinatário usa a chave privada para ler o conteúdo. *Um atacante pode interceptar e mudar o conteúdo, mas não pode ler.

Cripto (Autenticidade) - Assinatura digital

- Remetente usa chave privada p/ assinar (criptografar), gerando um hash criptografado da mensagem. (Única)
- Dest. usa a chave púb. apenas para ver a mensagem e analisar se houve alteração na mensagem, vendo o hash original e final. Verificação do Hash.

Cripto (Ambos)

- Alice escreve algo e gera um hash cripto. com a chave priv. dela, depois criptografa toda a mensagem c/ a pública de Bob.
- Bob usa a sua privada para ver a mensagem inteira e depois verifica o hash com a pública de Alice.

Pública:

- Gerada a partir da privada.
- Gerada de forma aleatória.

O RSA se baseia no problema de fatoração de n° muito grandes. O atacante precisa descobrir p e q apenas vendo n ($n=p \cdot q$).

MACETES PARA EUCLIDES:

Passos para calcular:

- ↳ P e Q ; $n = P \times Q$
- ↳ Função totiente de Euler $\phi(Z) = (P-1)(Q-1)$
- ↳ chave pub; $(n, e) \rightarrow e$ coprimo de Z , $MDC(e, Z)$ para verificar, $MDC = 1$
- ↳ chave priv. $-(n, d)$ Algoritmo Euclides: $\text{máximo divisor comum}$
 - ex: $mDC(120, 36)$

120 36	3	3	\rightarrow Quociente	36 12
-108 3	120 36	12		-36 3
12 //	12	0	\rightarrow Resto	0

Algoritmo de Euclides $A = (a, b)$ onde $a > b$

- 1º recebe o 120 e o 36 no meio
- 2º Realiza a divisão e coloca o quociente e o resto no lugar indicado
- 3º O resto vai para embaixo do 120 e depois no lado do 36. Pois vamos usar o 12 para achar o próx. n°
- 4º Para só quando chegar no resto 0.
- 5º O último do meio é o valor de $MDC(A)$ onde $A = (a, b)$
- 6º Após chegar em 0, montar a expressão de Euclides
 $\rightarrow \text{Dividendo} = \text{divisor} \cdot \text{Quociente} + \text{resto}$

Fórmula chave pública: $X = gx(\text{mod } n)$ (X chave pub; x n° secreto)

Chave intermediária: $Z' = ZX(\text{mod } n)$ (Z' chave int; Z chave púb. recebida; X n° secreto)

C. Secreta: $K = YX(\text{mod } n)$ (K chave sec.; Y chave int. recebida; X n° secreto)

Chave Pública

Chave Intermediária

$$X_m = 3^3 \pmod{11} = 5 \quad Z_m = 9^3 \pmod{11} = 3$$

$$X_j = 3^8 \pmod{11} = 3 \quad Z_j = 5^8 \pmod{11} = 4$$

$$X_c = 3^7 \pmod{11} = 9 \quad Z_c = 3^7 \pmod{11} = 9$$

Chave Secreta $\rightarrow K_m = 9^3 \pmod{11} = 3 \quad K_j = 5^8 \pmod{11} = 4 \quad K_c = 3^7 \pmod{11} = 9$

Cálculo mensagem RSA

Considerando $p=7$, $q=5$, temos $m=17$ e $e=5$.

FÓRMULAS:

- **Assinatura (cripto):** $s = m^d \pmod{n}$ (assinatura) $c = m^e \pmod{n}$ (cripto)
- **Verificação (decripto):** $m' = s^e \pmod{n}$ (verif) $m = c^d \pmod{n}$ (decript)

Exemplo:

Se $n=35$ e $z=24$. $(5 * d) \pmod{z} = 1$ $(5 * d) \pmod{24} = 1 \rightarrow$ Acha d por euclides ou testa valores.

Se $d=5$, **Assinatura:** $s = m^d \pmod{n} \Rightarrow s = 17^5 \pmod{35} \Rightarrow s=12$ **Verificação:** $m' = s^e \pmod{n} \Rightarrow m' = 12^5 \pmod{35} = 17 \checkmark$

Criptografia Clássica

Refere-se às técnicas de codificação usadas antes da computação moderna. Comunicação protegida para apenas entes que possuem ler, tornando inteligível apenas para aqueles que conheciam a chave. As técnicas eram divididas em:

- **Cifra de Substituição:** Substitui caracteres por outros com base em uma regra (tabela), ex: César, Vigenère, Hill.
- **Transposição:** Mantém os caracteres, mas reorganizam sua posição. Ex: Colunar, Rail Fence, Permutação de blocos.

Tabela Substituição

Contém os caracteres que serão substituídos pelos caracteres de substituição. A tabela também é chamada de cifrante. Quando apenas um cifrante é aplicado, é chamado de mono-alfabética.

C. CESAR

Veio de Roma antiga, mono alfabética, simples. (Baixa segurança, criptoanálise é quebrável por tentativa e erro e análise de frequência). $ABC \rightarrow DEF$ (3 casas). Vai testando deslocamentos de 1 a 25.

C. Vigenére

Século XVI, polialfabética, baseada em múltiplas deslocamentos definidos por uma palavra-chave, ex: média. Se a palavra-chave for fácil, é fácil quebrar usando criptoanálise de freq. de colunas. Usa uma tabela padrão com deslocamentos com linhas e colunas.

Texto plano: cacharro **Chave:** LIMALIMA (mesmo tamanho do texto, sempre) $C, L \rightarrow 1^\circ$ caractere do texto (Linha), 1° caractere chave (Coluna).

Transposição

Reorganiza/embaralha mantendo as letras.

COLUNA: Uma das técnicas mais primitivas de embaralhamento. Reversível, basta saber o nº de colunas. Baixa segurança, criptoanálise \rightarrow análise de frequência e tentativa de transposição. (Ver número e nome da coluna e a palavra e colocaram linha seguindo a sequência e depois pega as letras da coluna).

CACHORRO BONITO Pode usar chaves para decidir a ordem. Ex:

3 1 2

C A C

H O R \rightarrow [CHROT] [AOONO] [CRBIX]

R O B

O N I

T O X

Ordem: 3 1 2 (chave) CHROTAOONOCRBIX -> **AOONOCRBIXCHROT**

LICURGO

A técnica mais antiga usada pelos espartanos, é usada uma fita enrolada a um bastão (cítala) e escreve a mensagem na fita nas faces da cítala. Baixa segurança, criptoanálise e frequência de ocorrência das letras da língua.

ATUAIS

O DES utiliza um algoritmo de cifragem de transposição. O primeiro passo após informar a chave de 98 bits e 8 por 8 e o bloco de 64 bits. Com padding é transformar a chave principal em 16 subchaves (48 bits). Para isso é feito uma transp. de bits, uma permutação (PC-1), um embaralhamento dos 56 bits. Após isso, esses bits passam por uma rotação de bits à esquerda.

CRIPTOANÁLISE

Ciência de quebrar/hackear uma mensagem cifrada por meio da análise de padrões/ferramentas.

Processo de Cifra DES

Bloco

Uma mensagem dividida em blocos de 64 bits. Sofre uma permutação.

- Bloco dividido em 2 partes de 32 bits: L e R. → Apenas mudanças seguindo Feistel.
- R sofre expansão E (não) de 32 para 48 bits usando uma permutação fixa, permitindo que possa ser combinada c/ a subchave.
- O bloco expandido é combinado com a subchave através do XOR. Subchave derivada da chave principal (56 bits).
- **S-Boxes:** O resultado XOR (48 bits) é dividido em 8 blocos de 6 bits e cada bloco passa pela S-Box devolvendo 8 blocos de 4 bits → 32 bits no total, feito por uma tabela predefinida.
- Resultado passa por uma permutação e depois esse resultado é unido com L usando XOR, gerando a R criptog. de 32.
- Depois ocorre uma alteração entre L e R. Nova R: LR (64) → RL (64) → R vira L, L vira R. Vai sofrer as mesmas alterações.
- O processo se repete 16x.

Chave

Remove 8 bits de paridade, ficando 56 bits.

- **PC-1:** a chave passa por uma permutação fixa.
-

Criptografia DES

Quanto maior a aleatoriedade da chave, maior a segurança.

Desvantagens da Cripto. Simétrica:

- Todos na comunicação precisam conhecer a chave secreta.
- Problema de gerenciamento e distribuição das chaves.

Cifra de Bloco

A mensagem é dividida em blocos, no caso, de 64 bits. Cada bloco sofre um processo de cifra.

Cifra de Fluxo

A mensagem "OLÁ" possui 8 bits cada caractere. A chave vai cifrar de modo que mexa bit a bit, ou byte a byte da mensagem original.

CIFRA FEISTEL em DES

O algoritmo DES utiliza da cifra de Feistel para que cifrar use substituição e transposição (Permutação) dos elementos em 16 rodadas.

- É uma estrutura matemática e lógica para criar cifras de bloco.

Em 1970: Governo EUA exige um padrão de criptografia

Em 1977 a NSA adota a proposta de "Lucifer" da IBM de tamanho de chave 128 p/ 56 bits e torna a DES como padrão.

CARACTERÍSTICAS

Simétrica (mesma chave, tamanho p/ C e D). Não linear (saída totalmente diferente da entrada). Fácil implementação, chave com 56 bits (64 bits, mas tem 8 p/ paridade = 56).

Divisão da chave em 2: 28 bits (C e D)

- Ambas as partes sofrem rotações de bits à esquerda.
- O nº de rotações depende da rodada.
- **PC-2:** Ocorre uma permutação e compressão de 56 bits para 48 bits, gerando a subchave usada em cada uma das 16 rodadas.

Suspeitas:

- Nº baixo da chave, possibilitando força bruta (tamanho baixo).
 - Possível backdoor da NSA (achismos).
 - Nº de rodadas.
 - Falha de transposição.
-

Algoritmo RSA - Chave de 512 - 2048

Criptografia Assimétrica:

Par de chaves, tamanho de 512 a 4096 bits.

- Centros/Lojas das chaves e a aleatória, o resto calculado em função da 1ª.
- RSA: Usa criptografia com cálculos complexos sem transposição/subst.
- Usa o produto de números primos grandes com tamanho entre 100 e 200 dígitos. Usado em vários criptosistemas.

Criptosistema Confidencialidade (Sigilo):

- **Destinatário A cria as chaves:** Privada e pública e o remetente B recebe a chave pública.
- O remetente B escreve uma carta e criptografa com a chave pública de A.
- O destinatário A descriptografa usando sua chave priv.

C. Autenticidade (Assinatura digital com hash):

- B gera um par de chaves pub. e priv. B cria a mensagem e gera um hash da mensagem (resumo único por uma função hash SHA-256).
- B cifra o hash com sua chave priv. (Ass. digital).
- A usa a chave púb. de B p/ decifrar e verificar a mensagem.

Ambos:

(União de tudo e cada pessoa possui um par de chaves).

RSA:

Se baseia na fatoração e log. discreto. Fatoração difícil.

COMEÇANDO OS CÁLCULOS:

$n = p \cdot q$ (p, q são primos) c. Púb = (n,e) c. Priv = (n,d)

F. Euler: $z = (p-1)(q-1)$ Escolher e; $e < n$, coprimo de z e maior que 1. Escolher d; $e \cdot d \pmod{z} = 1$.

