Marisangila Alves, MSc
marisangila.alves@udesc.br
marisangila.com.br

UDESC
UNIVERSIDADE DO ESTADO DE SANTA CATARINA
JOINVILLE
CENTRO DE CIÊNCIAS TECNOLÓGICAS

UDESC
Universidade do Estado de Santa Catarina

2025/2

Segurança da Informação

Criptografia

Sumário

Introdução

> *A matemática é perfeita; a realidade é subjetiva. A matemática é definida. Os computadores são teimosos. A matemática é lógica; as pessoas são irregulares, caprichosas e pouco compreensíveis.*
>
> (SCHNEIER, 2001)

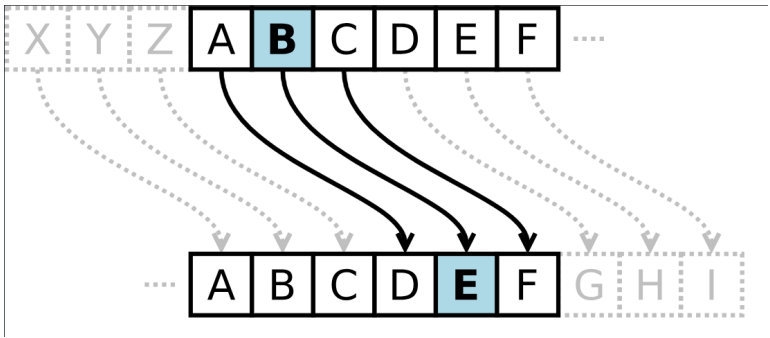
Definição

do inglês: crypto; do grego $\kappa\rho\upsilon\pi\tau o\varsigma$ - *kryptós*.
associado à idéia de algo escondido ou secreto (Etimologia, 2024).

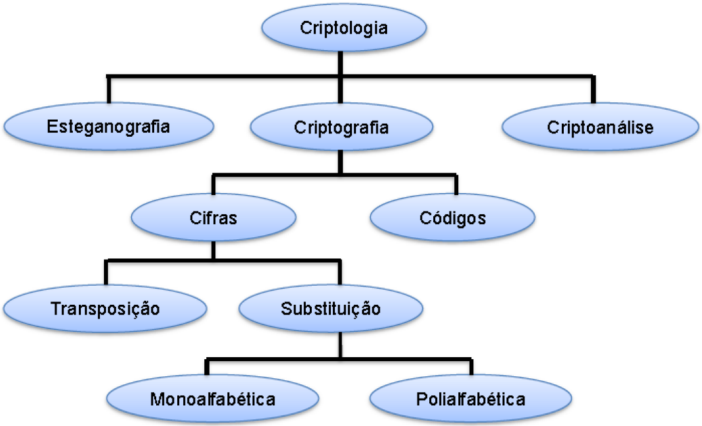
Nesse momento, abordaremos a criptografia como mecanismo de CONFIDENCIALIDADE!

> *A criptografia não é uma panecéia; você precisa de muito mais do que criptografia para ter segurança; mas é essencial. Para entender cibersegurança você precisa entender criptografia.*
>
> (SCHNEIER, 2001)

- Primeito uso documentado: 1900 a.C., no Egito;
- Registro na Mesopotâmia: 1500 a.C.;
- Cifra hebraíca: 500-600 a.C.;
- Cifra de César: 50-60 a.C; Uma das cifras histórica. A ideia é simples: deslocar cada letra por um determinado número para criptografar a mensagem.


X Y Z A B C D E F
A B C D E F G H I

- **Texto claro**: É a mensagem ou dados originais;
- **Texto cifrado**: É a mensagem embaralhada;
- **Cifrar ou encriptar**:Converter um texto claro em um texto cifrado;
- **Decifrar ou decriptar**: Restaurar o texto claro a partir do texto cifrado;
- **Chave Secreta**: Gerada pela encriptação e usado para decriptar.
- **Criptografia**:Área de estudo dos esquemas da encriptação.
- **Criptoanálise**: "Quebrar o código".
- **Criptologia**: Área de estudo que agrega criptografia e criptoanalise;



Formas de ataque a cifras:

Força Bruta

- Tentar todas as chaves possíveis em uma amostra de texto cifrado até obter tradução que leve a um texto às claras inteligível.
- A tabela mostra resultados para cada tamanho de chave, considerando que leva 1 s para executar uma única decifração, uma ordem de magnitude razoável.
- A última coluna da tabela considera os resultados para um sistema capaz de processar um milhão de chaves por microssegundo.

Key size (bits)	Number of possible keys	Time required for a decryption/μs	Time required for 10^6 decryption/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 Hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years

Figura: Tempo médio para busca exaustiva (STALLINGS; BROWN, 2015)

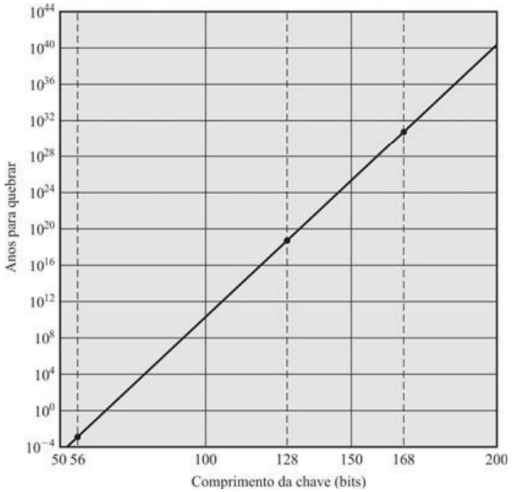


Figura: Tempo médio para busca exaustiva (STALLINGS; BROWN, 2015)

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Hive Systems

Read more and download at hivesystems.com/password

Syllabus

Ataque de senha mais comuns:

1. Força Bruta;
2. Dicionário;
3. Rainbow table;
4. Engenharia Social;

MUNDO

Sistema de segurança do Louvre é ultrapassado e tem falhas graves. A começar pela senha: Louvre

PUBLICADO 05/11/2025 • 08:38 | ATUALIZADO HÁ 4 DIAS

Da Redação

COMPARTILHAR

KEY POINTS

- O roubo das joias da coroa francesa no Museu do Louvre, avaliadas em cerca de US$ 102 milhões (aproximadamente R$ 500 milhões), expôs falhas de proteção em um dos museus mais renomados do mundo.
- O sistema de segurança, inclusive, usava apenas "Louvre" como senha de acesso.

Figura: Notícia Times Brasil sobre o roubo de jóais da coroa francesa no Museu do Louvre (Especulação).

Criptografia — © 2025 ALVES, M.

Criptoanálise

- Durante a Segunda Guerra Mundial, os alemães usaram a máquina de cifra **Enima** para codificar suas comunicações militares.
- **Alan Turing:** propos um método para quebrar seus códigos.
- A máquina "Bombe", projetada por Turing e sua equipe, foi essencial para descriptografar as mensagens codificadas pela Enigma.
- O trabalho de Turing e a quebra da Enigma impactaram significativamente na guerra.

CLICA!

Acesse um emulador Enigma
Acesse um emulador Bombe

1939

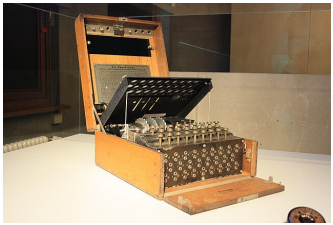


Figura: Enigma.

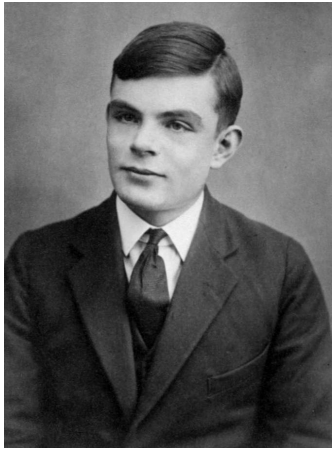


Figura: Allan Turing.

Figura: Bombe.

A criptoanálise requer raciocínio lógico!

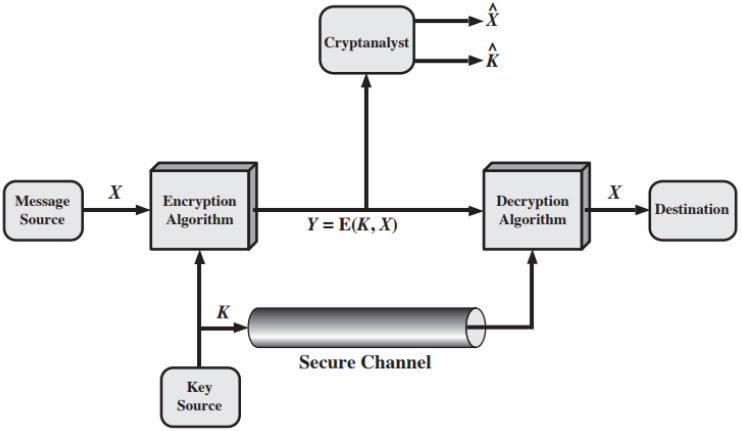
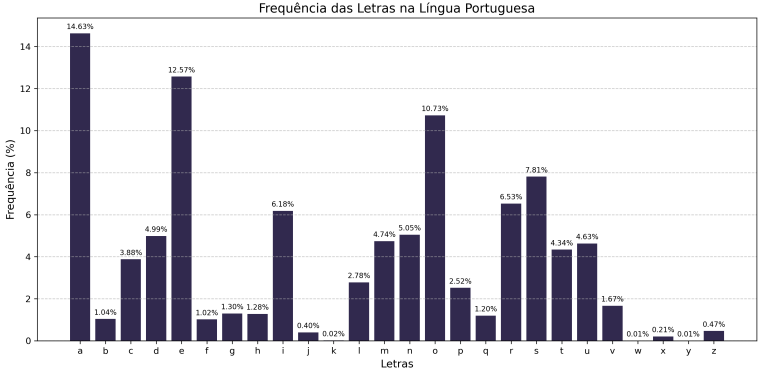


Figura: Criptoanálise (Stallings, 2020).

Figura: Exemplo de texto compactado (Stallings, 2020).

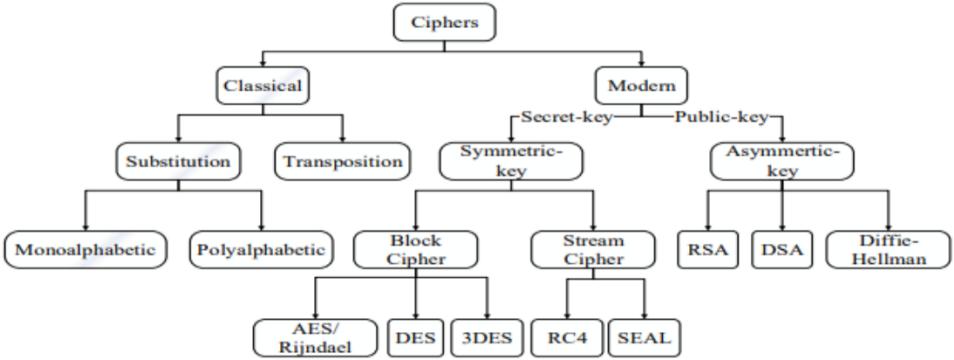
- Existe outra linha de ataque:
- Se o criptoanalista souber a natureza do texto claro (por exemplo. texto em inglês não compactado). O analis1a poderá explorar as regularidades da linguagem.

Em cifras de substituição, que trocam símbolos por outros, como a Cífra de César, é possível análisar a frequência dos símbolos.



Diferente das cifras de substituição, que trocam símbolos por outros, as cifras de transposição apenas **mudam a posição dos símbolos existentes**, preservando a frequência das letras.

Categoria	Cifra	Descrição / Característica principal
Substituição	**César**	Cada letra é substituída por outra deslocada no alfabeto por um número fixo. Ex.: A→D.
	Monoalfabética	Usa uma permutação fixa das letras do alfabeto — substituição simples de um-para-um.
	Polialfabética (Vigenère)	Emprega várias cifras de César em sequência, com base em uma palavra-chave.
	Playfair	Substitui pares de letras com base em uma matriz 5×5 derivada de uma chave.
	Hill	Usa multiplicações de matrizes modulares para substituir blocos de letras.
	Vernam (OTP)	Combina o texto claro com uma chave aleatória do mesmo tamanho via XOR. Se usada uma vez, é inquebrável.
Transposição	**Cítala**	Reorganiza letras ao escrever em volta de um bastão — cifra muito antiga.
	Colunas	Escreve o texto em linhas e lê em colunas conforme chave numérica.
	Rail Fence	Escreve o texto em zigue-zague e lê linha por linha.


Ciphers
Classical
Modern
Secret-key
Public-key
Substitution
Transposition
Symmetric-key
Asymmertic-key
Monoalphabetic
Polyalphabetic
Block Cipher
Stream Cipher
RSA
DSA
Diffie-Hellman
AES/ Rijndael
DES
3DES
RC4
SEAL

Esteganografia

Sentenças escritas guardam revelações escondidas, declaradas ocultamente.

Sentenças **E**scritas **G**uardam **R**evelações **E**scondidas,
Declaradas **O**cultamente.

SEGREDO

> *Uma mensagem em texto claro pode estar oculta de duas maneiras. Os métodos de esteganografia escondem a existência da mensagem, enquanto os métodos de criptografia a tornam ininteligível a estranhos por meio de várias transformações do texto.*
>
> (Schneier, 2015)

- Tintas invisíveis;
- Acrósticos;
- Perfurações;
- Bit menos significativo.


Imagem original
Informação confidencial
Imagem com a informação oculta

LSB: Least Significant Bits

Um dos métodos mais comuns e populares para esconder uma mensagem em uma imagem é a técnica de **LSB (Least Significant Bits)**. Esse método consiste em ocultar a informação nos bits menos significativos de cada byte do corpo da imagem.

Representação da imagem

Toda imagem digital é formada por:

- **Cabeçalho (header):** contém informações sobre formato, dimensões e metadados;
- **Corpo (body):** armazena os valores dos pixels (cores) em formato binário.

Um pixel RGB de 24 bits pode ser representado assim:

```
11101011 11000111 00000000
```

Red	Green	Blue
8 bits	8 bits	8 bits
11101011	11000111	00000000

Exemplo de inserção de mensagem por LSB

Temos três pixels:

```
pixel 1: 11101011 11000111 00000000
pixel 2: 01000010 10000110 11110100
pixel 3: 11110100 01010111 01000010
```

Queremos esconder o byte:

01100001

Alteramos os bits menos significativos (destacados em negrito):

```
pixel 1: 1110101{0} 1100011{1} 0000000{1}
pixel 2: 0100001{0} 1000011{0} 1111010{0}
pixel 3: 1111010{0} 0101011{1} 01000010
```

Criptografia — © 2025 ALVES, M.

Resultado:

- A mensagem foi escondida nos bits menos significativos;
- O pixel 1 mudou de #ebc700 para #eac701;
- A diferença visual é praticamente imperceptível.

Criptografia — © 2025 ALVES, M.

Extração da mensagem:
O processo inverso recupera os bits escondidos:

```
pixel 1: 1110101{0} 1100011{1} 0000000{1}
pixel 2: 0100001{0} 1000011{0} 1111010{0}
pixel 3: 1111010{0} 0101011{1} 01000010
-> mensagem: 01100001
```

01100001, em decimal: 97, na tabela ASCII: a

Técnica LSB - Least Significant Bit VI

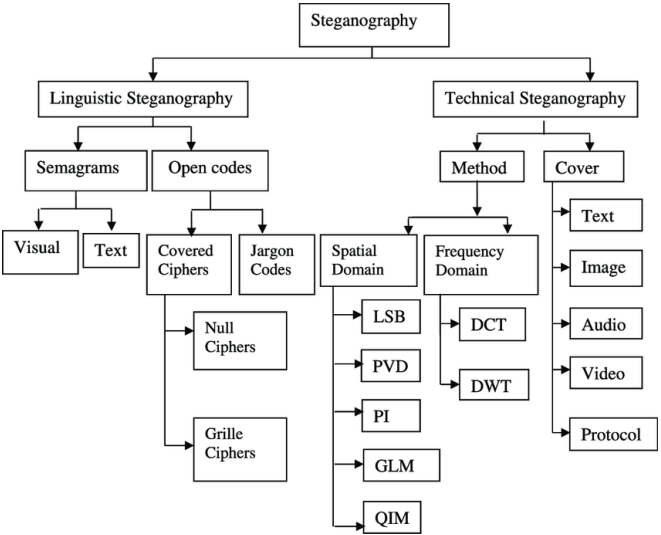


Imagem Full HD

A resolução de uma imagem Full HD (1.920 × 1.080 pixels) contém aproximadamente **2,07 milhões de pixels**, e cada pixel armazena **24 bits** de informação (8 bits para cada componente RGB).

- Se o bit menos significativo (LSB) de cada canal for alterado, a diferença é praticamente imperceptível ao olho humano.
- É possível ocultar até cerca de **750 kB de dados** em uma única imagem Full HD sem afetar significativamente sua qualidade visual.
- Ferramenta: **Steghide**.

Limitações

- Necessita de muito espaço para esconder uma pequena quantidade de dados.
- Quando o método é descoberto, perde sua eficácia, pois o conteúdo pode ser removido ou detectado.

Criptografia Simétrica

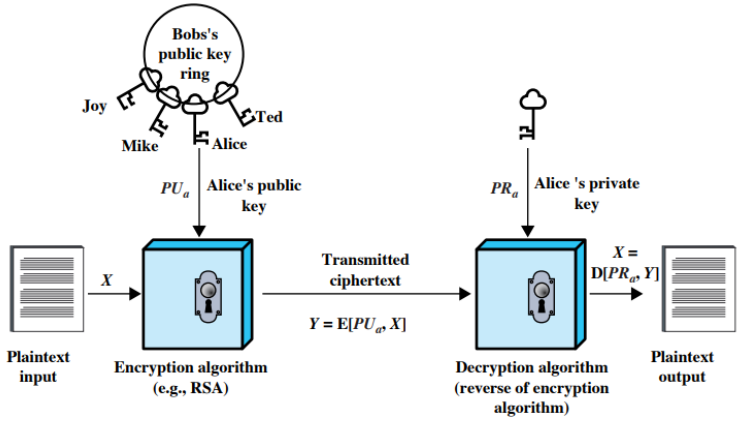


Figura: Modelo simplificado criptografia simétrica (Stallings, 2020)

- Algoritmo forte, ou seja, mesmo que o algoritmo e o texto cifrado são conhecidos, não é possível obter o texto claro ou a chave secreta.
- Remetente e destinatário devem obter cópias da chave secreta de maneira segura e mantê-las em segurança.

- DES foi adotado em 1977 pelo NIST.
- DES foi adotado como padrão em 1977 e usa uma chave de 56 bits. Com o avanço do poder computacional, em 1999, a DES a chave foi quebrada com sucesso em menos de 24 horas, motivando a mudança para o 3DES.
- 3DES é DES aplicado três vezes; consequentemente, o tamanho da chave é de 168 bits, embora a segurança efetiva seja de 112 bits.
- O 3DES foi descontinuado em 2019 e deve ser substituído por AES.

Característica	Cifra de Bloco	Cifra de Fluxo
Unidade de operação	Opera em blocos de tamanho fixo (ex.: 64 ou 128 bits).	Opera bit a bit ou byte a byte (fluxo contínuo).
Necessidade de Padding	Sim, para completar o tamanho do bloco.	Não, pois trabalha em fluxo contínuo.
Uso típico	Armazenamento de arquivos, bancos de dados, pacotes de rede.	Transmissões em tempo real (voz, vídeo, IoT).
Exemplos de algoritmos	**AES**, **DES**, **Blowfish**.	**RC4**, **Salsa20**, **ChaCha20**.

- **Troca Física:** A chave pode ser entregue manualmente, por exemplo, via pendrive ou outro meio fora da rede.
- **Servidor Confiável (Kerberos):** Um servidor central autentica as partes e distribui chaves de sessão simétricas.
- **Troca pela Rede (Criptografia Assimétrica):** É possível trocar chaves de forma segura utilizando algoritmos de **criptografia assimétrica**,

Matemática

Importância Matemática

A base da criptografia moderna está na matemática. Duas operações amplamente utilizadas em diversos algoritmos são:

- **Operação XOR (OU Exclusivo)**
- **Operação Módulo**

Operação XOR

XOR significa "OU Exclusivo" e é uma operação lógica em aritmética binária. Ela compara dois bits e retorna:

- **1** se os bits forem diferentes;
- **0** se os bits forem iguais.

A	B	A $\oplus$ B
0	0	0
0	1	1
1	0	1
1	1	0

Exemplo: $1010 \oplus 1100 = 0110$

Criptografia — © 2025 ALVES, M.

Propriedades do XOR

- $A \oplus A = 0$
- $A \oplus 0 = A$
- Comutativa: $A \oplus B = B \oplus A$
- Associativa: $(A \oplus B) \oplus C = A \oplus (B \oplus C)$

Essas propriedades tornam o XOR útil em **criptografia e detecção de erros**.

Uso do XOR na Criptografia

Podemos usar XOR como uma forma simples de criptografia simétrica:

$$C = P \oplus K$$

Onde:

- P = texto plano
- K = chave secreta
- C = texto cifrado

Para decifrar:

$$P = C \oplus K$$

Assim, aplicando XOR duas vezes com a mesma chave, recuperamos o texto original.

Operação Módulo

A operação **módulo**, representada por % ou `mod`, retorna o **resto da divisão** de dois números.

- $25 \bmod 5 = 0 \quad \Rightarrow 25 = 5 \times 5 + 0$
- $23 \bmod 6 = 5 \quad \Rightarrow 23 = 3 \times 6 + 5$
- $23 \bmod 7 = 2 \quad \Rightarrow 23 = 3 \times 7 + 2$

Propriedades:

- O resultado é sempre um valor entre 0 e $n - 1$.
- Não é reversível: múltiplos valores de x podem satisfazer $x \bmod n = r$.

Importância na Criptografia

A operação módulo é essencial em sistemas como o **RSA** e o **Diffie–Hellman**, onde operações de exponenciação e multiplicação são realizadas sob um número primo n, mantendo os resultados dentro de limites previsíveis e seguros.

Criptografia Assimétrica

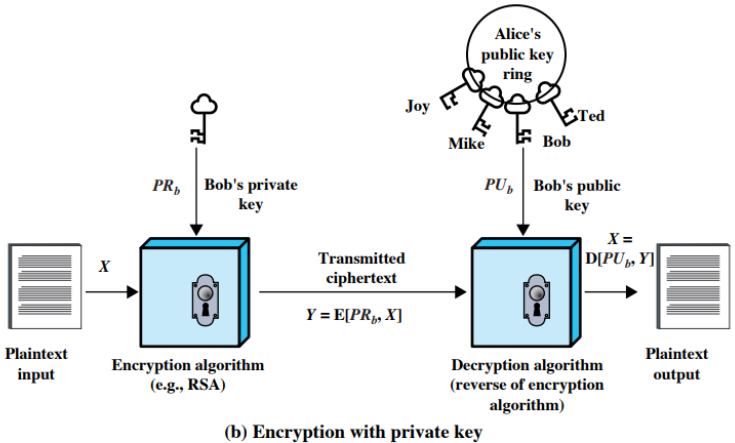
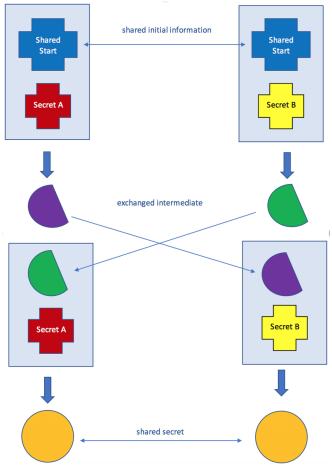
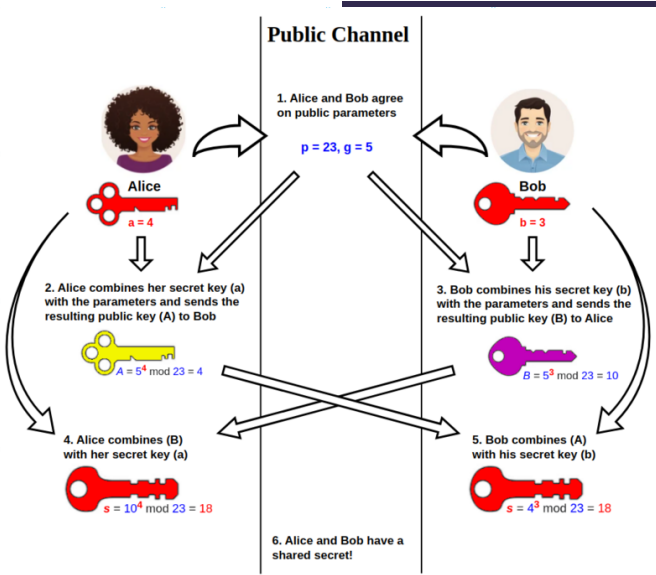


Figura: Criptografia assimétrica (Stallings, 2020)



Criptografia — © 2025 ALVES, M.


Public Channel
1. Alice and Bob agree on public parameters
p = 23, g = 5
Alice
a = 4
Bob
b = 3
2. Alice combines her secret key (a) with the parameters and sends the resulting public key (A) to Bob
A = 5^4 mod 23 = 4
3. Bob combines his secret key (b) with the parameters and sends the resulting public key (B) to Alice
B = 5^3 mod 23 = 10
4. Alice combines (B) with her secret key (a)
s = 10^4 mod 23 = 18
5. Bob combines (A) with his secret key (b)
s = 4^3 mod 23 = 18
6. Alice and Bob have a shared secret!

- Ele resolve o problema de como duas partes podem concordar em uma chave secreta sem enviá-la explicitamente.
- Após a troca, ambos calculam a mesma chave simétrica usando operações matemáticas (exponenciação modular).
- Mesmo que alguém intercepte todas as mensagens trocadas, não consegue derivar a chave secreta (baseado na dificuldade do problema do logaritmo discreto).

Origem

Diffie e Hellman introduziram uma nova técnica de criptografia que desafiou os criptologistas a criarem um sistema de chave pública. Em 1977, **Ron Rivest**, **Adi Shamir** e **Len Adleman**, do MIT, desenvolveram o **RSA**, publicado em 1978. Desde então, o RSA tem sido a técnica de uso geral mais aceita para criptografia de chave pública.

Geração das Chaves

1. Escolha dois números primos grandes e distintos, p e q.
2. Calcule o produto $n = p \times q$, chamado de **módulo**.
3. Calcule a função totiente de Euler: $\varphi(n) = (p-1)(q-1)$.
4. Escolha um inteiro e tal que $1 < e < \varphi(n)$ e que seja **coprimo** com $\varphi(n)$.
5. Determine d, o inverso multiplicativo de e módulo $\varphi(n)$, ou seja:

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

6. A chave pública é (n, e) e a chave privada é (n, d).

Criptografia

- Represente a mensagem como um número inteiro m, onde $0 < m < n$.
- Calcule o texto cifrado:

$$c \equiv m^e \pmod{n}$$

Descriptografia

- Calcule o texto original a partir do texto cifrado:

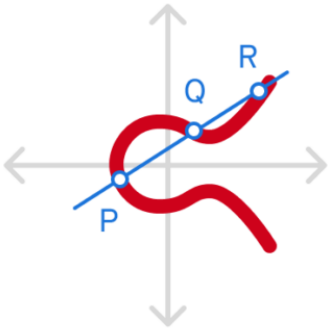
$$m \equiv c^d \pmod{n}$$

Base de Segurança

- A segurança do RSA se baseia na dificuldade de fatorar grandes números em seus primos constituintes.
- Fatorar um número grande significa encontrar os números primos que, multiplicados, formam o número original.
- Esse problema é considerado **intratável** para números suficientemente grandes, mesmo com os algoritmos mais avançados.

Implementação Prática

- Cada caractere é convertido para um valor numérico (ex.: ASCII) antes da aplicação do RSA.
- Para lidar com números muito grandes, utiliza-se **aritmética de precisão arbitrária (big integers)**.



$$y^2=x^3+ax+b$$

Criptografia — © 2025 ALVES, M.

- A criptografia de curvas elípticas (ECC) é baseada na dificuldade do **Problema do Logaritmo Discreto em Curvas Elípticas (ECDLP)**, considerado computacionalmente mais difícil que o logaritmo discreto clássico usado em RSA e Diffie–Hellman.
- Por isso, ECC oferece **o mesmo nível de segurança** que RSA usando chaves menores:
  - RSA seguro: **3072 bits** (segurança equivalente a 128 bits do ECDSA).
  - ECC/ECDSA seguro: **256 bits** (segurança equivalente a 3072 bits do RSA).

- **ECDSA** (Elliptic Curve Digital Signature Algorithm): usado para **assinaturas digitais**.
- **ECDH** (Elliptic Curve Diffie–Hellman): usado para **troca de chaves** de forma segura entre duas partes. Similar ao Diffie–Hellman clássico, porém usando operações sobre curvas elípticas.
- Em protocolos modernos (TLS 1.3, SSH, certificados ICP-Brasil, etc.), **ECC é preferida** por oferecer mais segurança com menos bits.

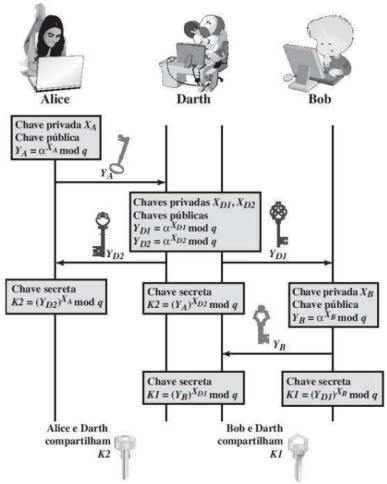


Figura: Chave Pública e ataque *man-in-the-middle* (Schneier, 2015)

VULNERABILIDADE

O protocolo de troca de chaves é vulnerável a tal ataque porque não autentica os participantes. Essa vulnerabilidade pode ser contornada com o uso de assinaturas digitais e certificados de chave pública.

- A criptografia assimétrica tende a ser mais lenta, e muitas cifras de criptografia assimétrica usam chaves maiores do que a criptografia simétrica. Por exemplo, RSA usa chaves de 2048 bits, 3072 bits e 4096 bits; 2048 bits é o tamanho mínimo de chave recomendado.

- A criptografia assimétrica é baseada em um grupo específico de problemas matemáticos que são fáceis de calcular em uma direção, mas extremamente difíceis de reverter. Neste contexto, extremamente difícil significa praticamente inviável. Por exemplo, podemos confiar em um problema matemático que levaria muito tempo, por exemplo, milhões de anos, para ser resolvido usando a tecnologia atual.

Além do serviço de CONFIDENCIALIDADE é possível usar criptografia de chave pública para AUTENCIDADE E ASSINATURA (NÃO REPÚDIO)!

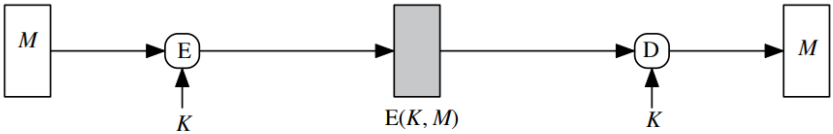
Criptografia Moderna

,

Notação

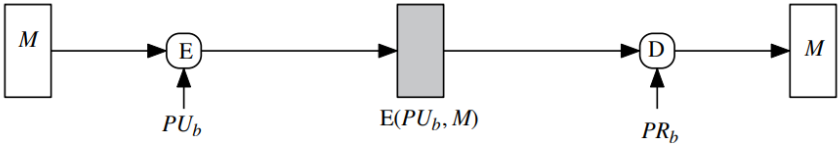
- $\mathbf{P}$ – Chave simétrica trocada entre entidades para (C) criptografar e (D) descriptografar (M) mensagens.
- $\mathbf{P_U}$ – Chave pública de uma entidade que pode ser usada para criptografar e descriptografar mensagens.
- $\mathbf{P_R}$ – Chave privada de uma entidade que pode ser usada para criptografar e descriptografar mensagens.

,



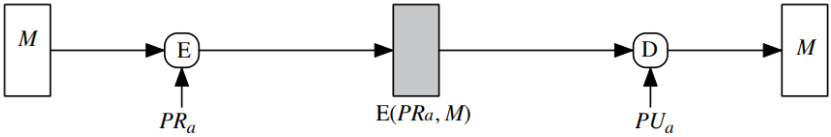
(a) Symmetric encryption: confidentiality and authentication

Figura: Simétrica: Confidencialidade e Autenticação (Stallings, 2020)



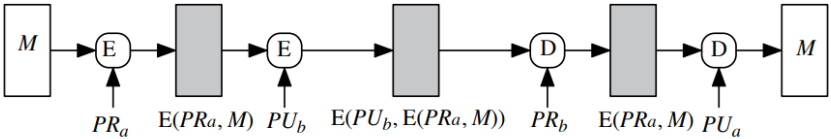
(b) Public-key encryption: confidentiality

Figura: Assimétrica: Confidencialidade (Stallings, 2020)



(c) Public-key encryption: authentication and signature

Figura: Assimétrica: Autenticação e Assinatura - Não repúdio (Stallings, 2020)



(d) Public-key encryption: confidentiality, authentication, and signature

Figura: Assimétrica: Confidencialidade, Autenticação e Assinatura (Stallings, 2020)

SCHNEIER, Bruce. **Segurança.com**. 1. ed. São Paulo: Campus, 2001.

STALLINGS, William. **Cryptography and Network Security: Principles and Practice**. 8. ed. [*S. l.*]: Pearson, 2020.

STALLINGS, William; BROWN, Lawrie. **Computer security: principles and practice**. 1. ed. São Paulo: Pearson Prentice Hall, 2015. p. 492. ISBN 9788576051190.

Licença

Licenciado sob CC BY-NC-ND 4.0.