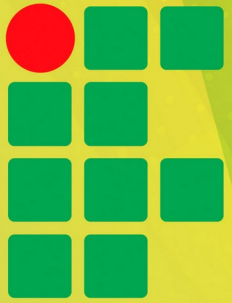
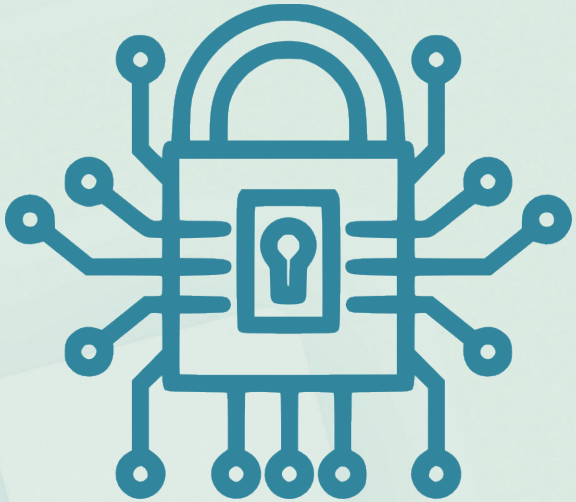


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação



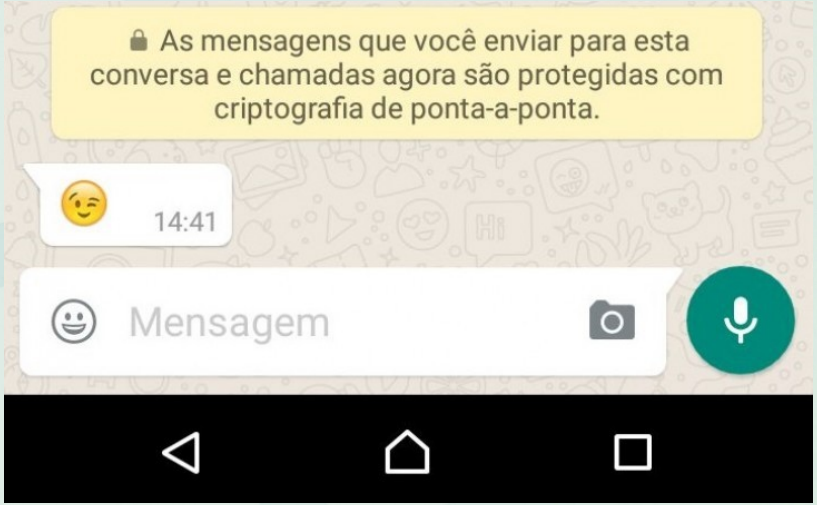
Criptografia

Prof. Heraldo Gonçalves Lima Junior

INSTITUTO FEDERAL
Sertão Pernambucano

1. Introdução

- Já percebeu que ao abrir uma nova conversa no WhatsApp você recebe uma mensagem dizendo que ela é criptografada?



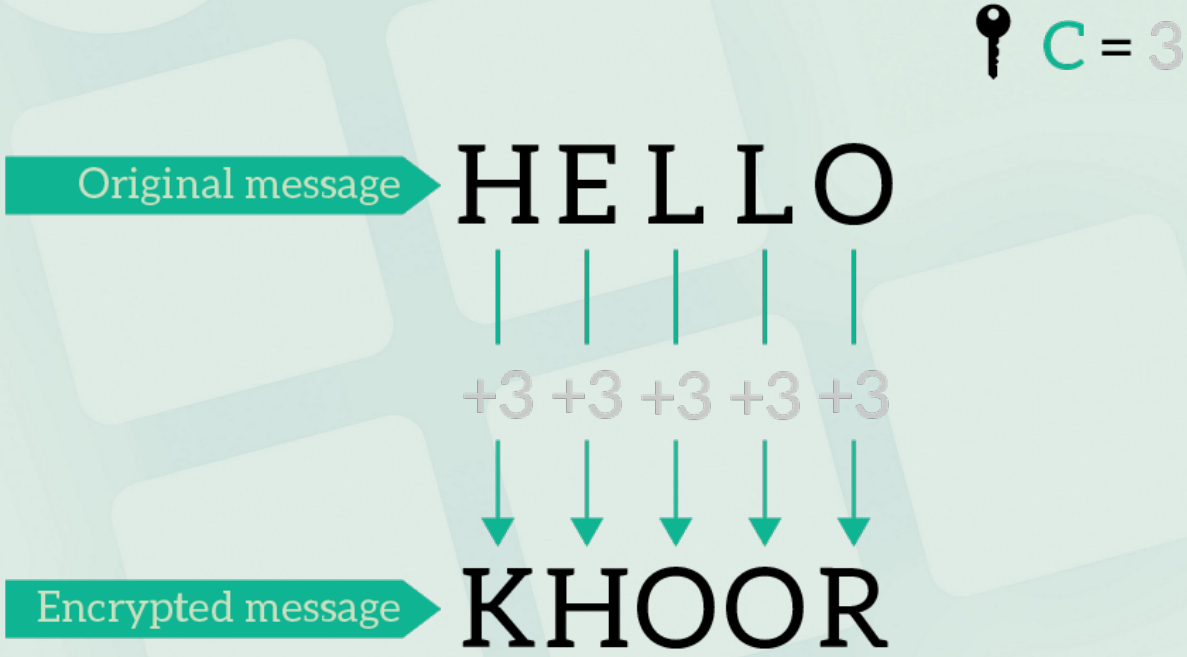
1. Introdução

- A criptografia é um conjunto de **técnicas pensadas para proteger uma informação** de modo que **apenas o emissor e receptor consigam compreendê-la**.
- É utilizada em comunicações digitais, como na troca de mensagens ou em pagamentos online.

1. Introdução

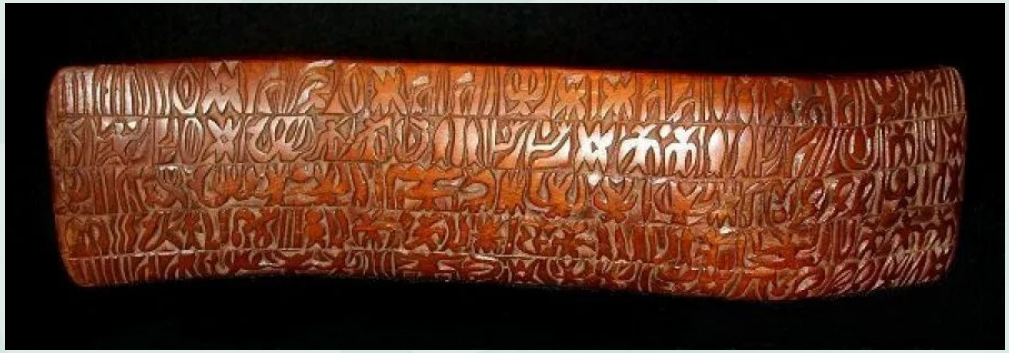
- Em geral são usados algoritmos para realizar o codificação e para decodificação é necessário ter acesso à chave utilizada no primeiro processo.

1. Introdução



2. História

- Estima-se que essa estratégia surgiu há cerca de 1.900 anos antes de Cristo, no Egito. Um exemplo de criptografia antiga é o Rongorongo, nunca foi decifrada.

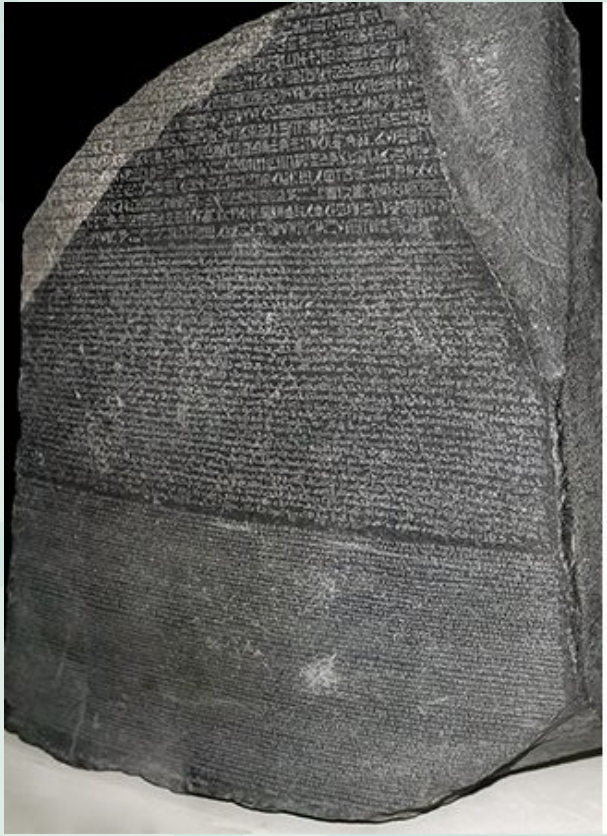


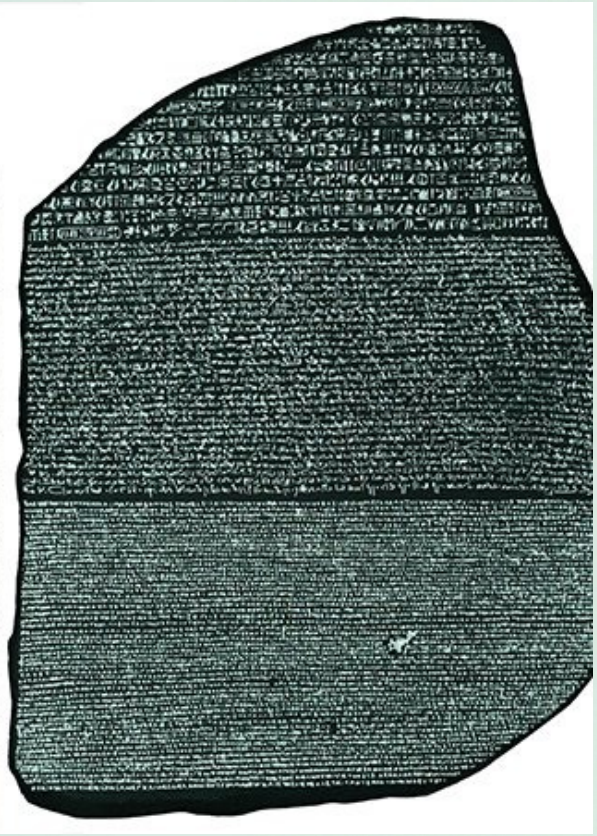
2. História

2. História

- Já um exemplo da origem da criptografia que foi desvendada é a famosa Pedra de Roseta.
- Encontrada no Egito em 1799, por tropas francesas comandadas por Napoleão Bonaparte, o pedaço de granito é coberto pelo mesmo texto, mas em 3 diferentes grafias/idiomas.

2. História





2. História

- Já um exemplo da origem da criptografia que foi desvendada é a famosa Pedra de Roseta.
- Encontrada no Egito em 1799, por tropas francesas comandadas por Napoleão Bonaparte, o pedaço de granito é coberto pelo mesmo texto, mas em 3 diferentes grafias/idiomas.

3. Chaves e Protocolos

- Atualmente, **a base da criptografia simétrica e assimétrica são as chaves**, que podem ser utilizadas para criptografar e também para descriptografar informações.

- Alguns exemplos de protocolos são: **DES, 3DES, AES, IDEA, RC4, TLS e SSL.**

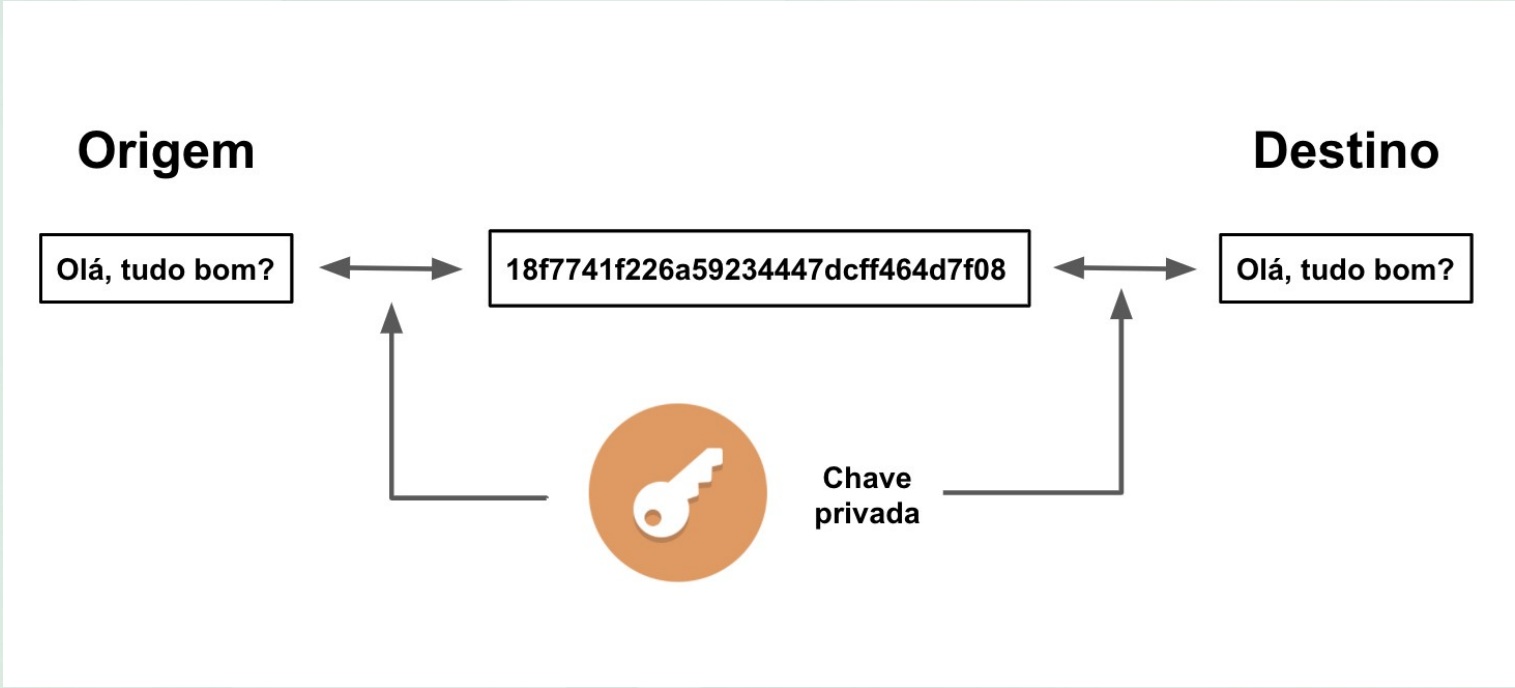
3. Chaves e Protocolos

- Existem também protocolos de criptografia que não utilizam chaves, chamados de algoritmos de **HASH**.

3.1. Criptografia simétrica

- A criptografia simétrica é o tipo mais tradicional e provavelmente o sistema que as pessoas estão mais familiarizadas.
- Nele, a criptografia **é realizada com base em uma única chave — que é utilizada para criptografar e também descriptografar uma mensagem.**

3.1. Criptografia simétrica



3.1. Criptografia simétrica

- Sua principal aplicação é na **proteção de dados em repouso**, como em bancos de dados ou discos rígidos — isso porque é necessário contar com um canal seguro para transmitir a mensagem.

3.1. Criptografia simétrica

- **Vantagem:** mais rápida e ideal para proteger dados que vão ficar em único local.

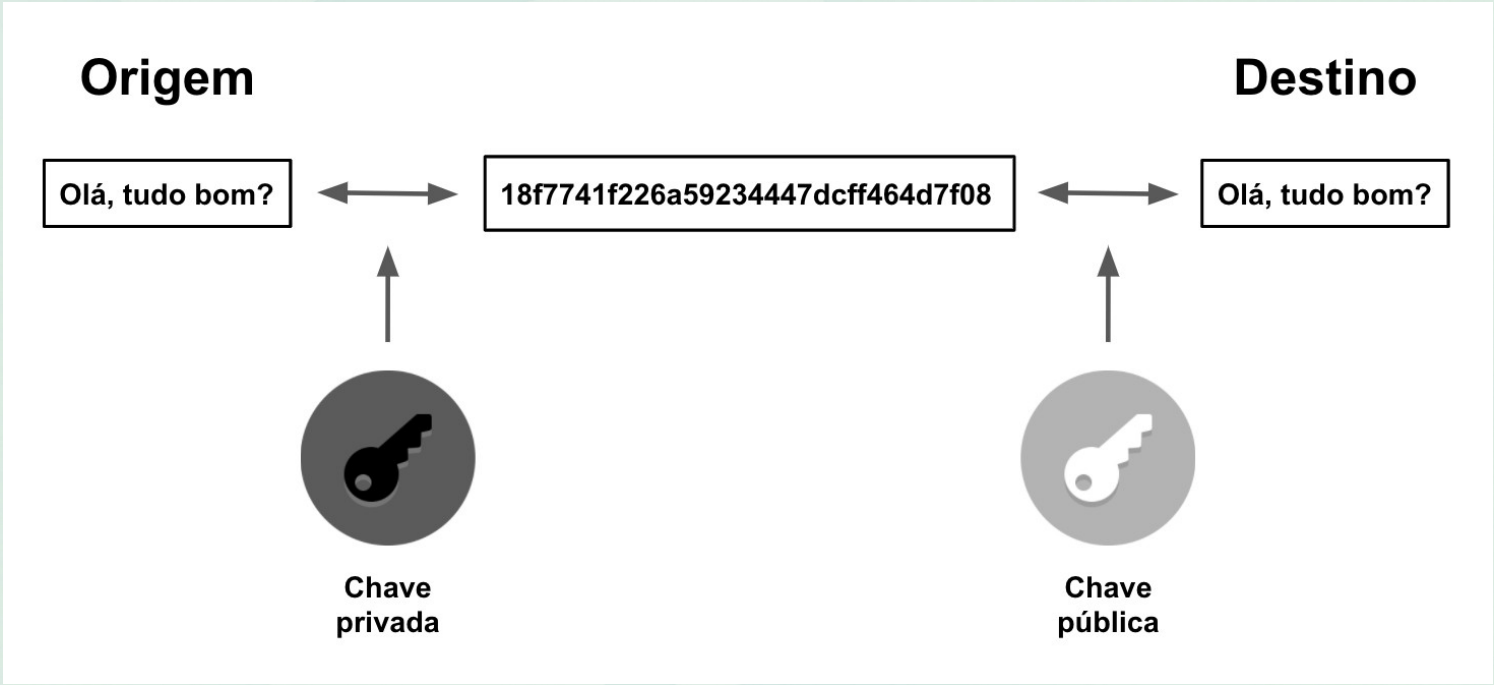
- **Desvantagens:** dificuldade de distribuição segura de chaves.

3.2. Criptografia assimétrica

- A criptografia assimétrica utiliza duas chaves diferentes para criptografia e descriptografia de um dado.

- A primeira chave é uma chave pública usada para criptografar uma mensagem e a segunda é uma chave privada utilizada para descriptografá-la.

3.2. Criptografia assimétrica



3.2. Criptografia assimétrica

- **Apenas uma chave privada pode descriptografar as mensagens criptografadas por uma chave pública.**
- A criptografia assimétrica é aplicada em várias operações do dia a dia, **como assinatura eletrônica, envio de e-mails** ou mesmo realizar uma **conexão remota a um sistema privado.**

3.2. Criptografia assimétrica

3.2. Criptografia assimétrica

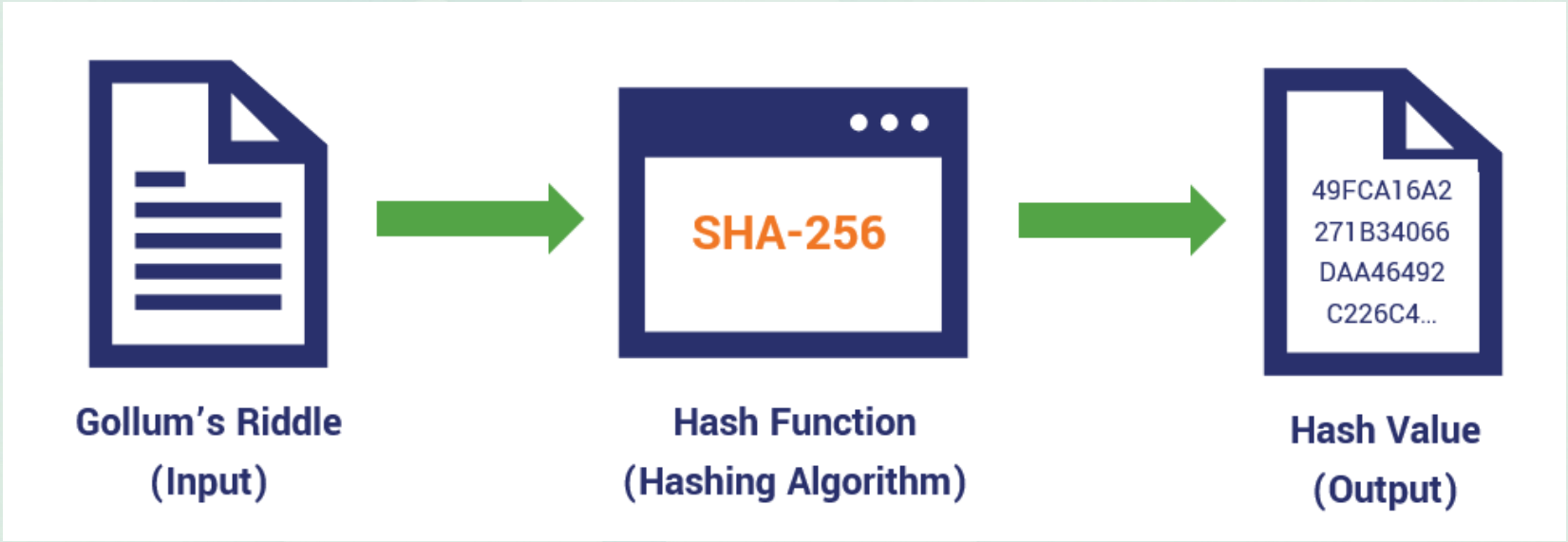
- **Vantagens:** as pessoas não precisam de nenhum esquema de segurança específico para trocar mensagens com confidencialidade.

- **Desvantagens:** É mais lenta.

3.3. Hashing

- **Embaralha os dados de forma que sejam sequer reconhecíveis**.
- A única diferença para o tipo simétrico e assimétrico, é que o hashing não foi projetado para ser reversível.

3.3. Hashing


SHA-256
49FCA16A2
271B34066
DAA46492
C226C4...
Gollum's Riddle
(Input)
Hash Function
(Hashing Algorithm)
Hash Value
(Output)

3.3. Hashing

- É uma função matemática aplicada sobre um determinado tipo de dado, que gera assim outro número único.
- **O hashing é utilizado na:**
- Geração de **assinaturas digitais**;
- Análise e **verificação da validade e integridade** de arquivos digitais.

3.3. Hashing

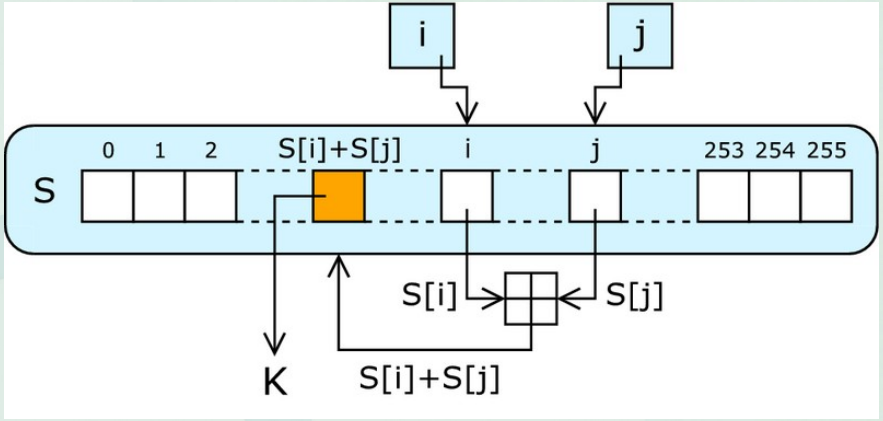
- A finalidade do hashing não é necessariamente ocultar o conteúdo de uma mensagem, por exemplo, mas sim verificar sua integridade.

4. Principais algoritmos criptográficos

- A criptografia, apesar de ser resumida em poucos tipos, possui vários algoritmos: tanto simétricos, quanto assimétricos.
- **Talvez você se pergunte: “porque existem tantos algoritmos diferentes?“**

4.1. RC4

- A criptografia RC4, sigla para Rivest Cipher 4, é uma cifra de fluxo (stream cipher) criada no fim dos anos 1980, um algoritmo simétrico.

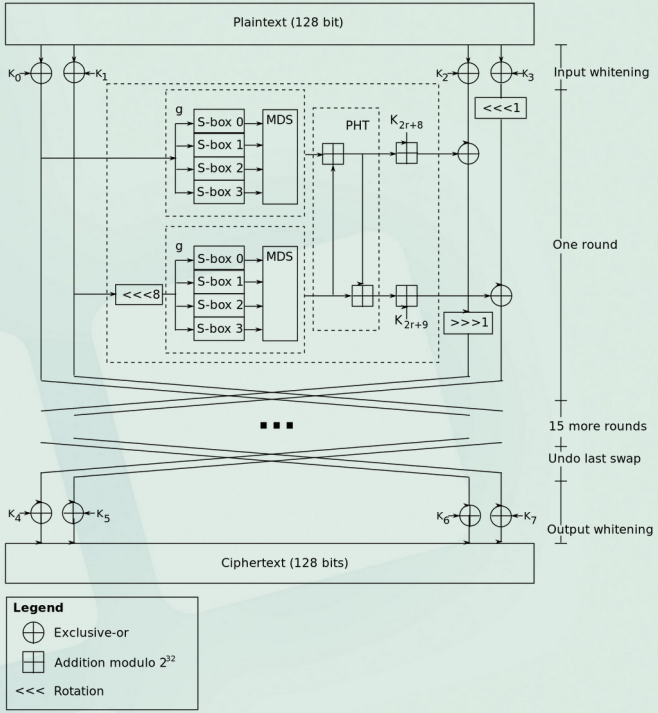


4.1. RC4

- Essa cifra opera nos dados **um byte por vez**, de modo a criptografar esses dados.
- O RC4 é uma das cifras de fluxo mais usadas, tendo sido usado nos protocolos **Secure Socket Layer (SSL)** — hoje conhecido como **Transport Layer Security (TLS)**.

4.2. Twofish

- Outro tipo de criptografia simétrica é a Twofish, uma evolução da Blowfish — sendo assim, apenas uma chave de 256 bit é necessária.

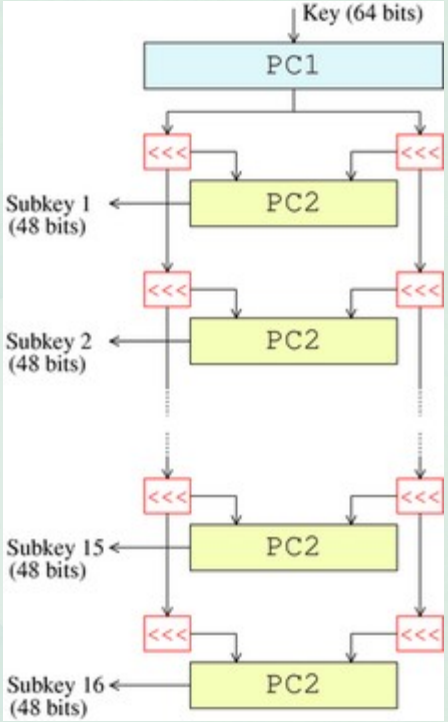


4.2. Twofish

- É bastante útil e segura, sendo finalista de uma competição do Instituto de Tecnologia e Ciências Nacional americano, que buscava uma criptografia para substituir a DES.

4.3. DES

- A criptografia DES, sigla para Data Encryption Standard, é também um tipo de chave simétrica — um dos primeiros que foi criado, datando do começo da década de 1970, por um time de desenvolvedores da IBM.



4.3. DES

- Converte texto simples em blocos de 64 bits em texto cifrado, com chaves 48 bits.
- Por conta do tamanho pequeno da chave, ele é considerado inseguro para várias aplicações atualmente.
- Hoje, o DES foi substituído pelo AES.

4.4. RSA

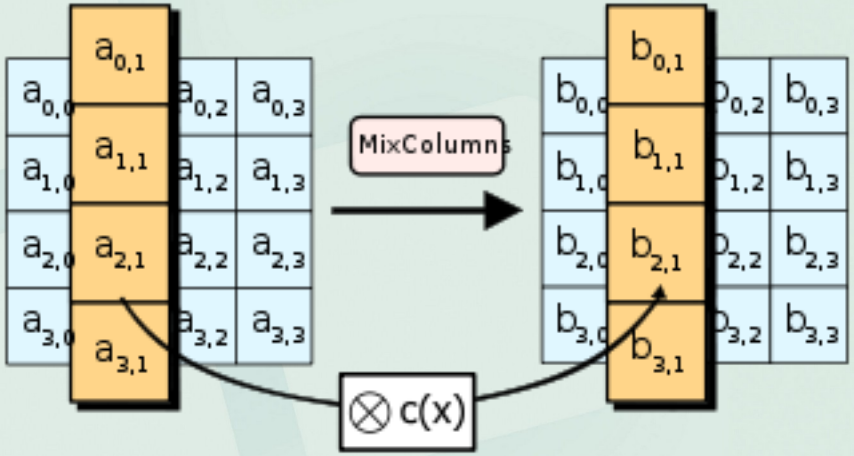
- Já a criptografia RSA é um tipo assimétrico. A sigla diz respeito ao nome de seus criadores, Rivest-Shamir-Adleman.
- Ele é muito utilizado hoje em dia e seu funcionamento tem a mesma explicação da criptografia assimétrica.

4.5. AES

- Já a criptografia AES ou Advanced Encryption Standard é um tipo de cifra que **protege a transferência de dados online**.
- É um dos **melhores e mais seguros protocolos de criptografia** e é utilizado em incontáveis aplicações.

4.5. AES

- Na prática, é uma chave simétrica, pois utiliza a mesma chave para criptografar e descriptografar o conteúdo.



5. Anonimização, pseudonimização e criptografia

- **Anonimização:** desassociar informações de indivíduos.
  - Nesse tipo de situação, pode-se utilizar os algoritmos de HASH mencionados anteriormente.

5. Anonimização, pseudonimização e criptografia

- **Pseudoanonimização:** Também é uma forma de não atribuir informações a indivíduos, sem recorrer a informações suplementares.
- É um processo reversível, podendo ser futuramente atrelado aos dados para voltar a identificação do indivíduo.

6. Benefícios da criptografia

- A criptografia ajuda a **manter a integridade dos dados.**
- Ajuda as organizações a **cumprir as regulamentações**

6. Benefícios da criptografia

- Protege os **dados entre dispositivos**
- Ajuda ao **mover dados para armazenamento em nuvem**.

6. Benefícios da criptografia

- Ajuda a **proteger os escritórios virtuais e a propriedade intelectual**.

7. Como é feita a criptografia

- Fazer uma criptografia **vai depender do objetivo** que você tem em mente.
- No caso de uma empresa, o uso de um servidor de e-mails como o **Gmail**, por exemplo, já garante que as comunicações por esse canal estarão criptografadas.

8. Criptografia homomórfica

- O principal objetivo deste tipo de codificação é poder **realizar operações diretamente sobre os dados criptografados**, sem necessidade de descriptografá-los previamente ou de dispor da chave com que foram criptografados.

8. Criptografia homomórfica

8. Criptografia homomórfica

- Um detalhe impressionante é que os algoritmos de criptografia mais comuns **são normalmente concebidos para não ter propriedades de homomorfismo** para que os dados criptografados **não tenham uma estrutura relacionada com os dados originais**.

8. Criptografia homomórfica

- Seu uso pode ser benéfico na gestão de dados médicos, sistemas de votação eletrônica, sistemas de computação forense e especialmente para serviços encadeados ou centrados na nuvem.

8. Criptografia homomórfica

- O desafio em alguns tipos de serviço é o **elevado volume de dados e que estes devem ser transmitidos criptografados para, em seguida, serem descriptografados** – permanecendo neste ponto vulnerável – durante o processamento num servidor externo. **Como garantir a integridade?**

8. Criptografia homomórfica

- É por isso que este tipo de situação é ideal para o uso de criptografia homomórfica. Assim, os usuários acessam os arquivos sem a possibilidade de modificar sua integridade.

8. Criptografia homomórfica

INSTITUTO FEDERAL
Sertão Pernambucano

Obrigado!
Vlw! Flw!

INSTITUTO FEDERAL
Sertão Pernambucano