SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE II – IMPLEMENTAÇÃO DA SEGURANÇA NOS DADOS

PUC Minas
Virtual

2.2 – SERVIÇOS E TÉCNICAS DE AUTENTICAÇÃO

PUC Minas
Virtual

2.2.2 – TÉCNICAS DE CRIPTOGRAFIA

SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

- Até pouco tempo atrás, a criptografia era sinônimo de encriptação, que é o processo de **converter um texto comum** (ou texto em claro) para um **texto inelegível** (ou **cifra**).
- Existem duas formas mais **modernas** para se encriptar os dados, ou arquivos e que são utilizados para proteger a transmissão no meio físico.
- Iniciamos nossa jornada falando sobe métodos de substituição que possuem um **defeito:** caso quem deseja conhecer a mensagem tenha o conhecimento de médio para alto do idioma da qual a mensagem foi codificada pode realizar testes de substituição de caracteres e, por repetição, encontrar palavras e assim deduzir outros caracteres codificados.

SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

- Atualmente, a necessidade de criptografar passou de mensagens cruzadas entre duas partes para a proteção de inúmeros elementos como arquivos de fotos ou de outro tipo.
- Junte-se a isto à evolução tecnológica da era dos microchips e à base de codificação que são os algoritmos matemáticos.
- **Poder de processamento** na execução dos cálculos e **cálculos mais complexos** que nas tecnologias anteriores.
- Se a técnica não muda, a potência de cálculo necessária, através de teste e erro, acaba finalmente descobrindo a informação oculta por trás de uma mensagem codificada.

OBJETIVOS DA CRIPTOGRAFIA

- **Confidencialidade:** somente o destinatário autorizado da mensagem consegue extrair o conteúdo e entender a mensagem. Pode ser entendida como um cofre e quem tem a chave é que tem acesso ao conteúdo do cofre;
- **Integridade:** somente o destinatário consegue verificar se a mensagem foi alterada durante a transmissão e esta ação é feita como garantia que alguém malicioso não envie alguma mensagem correta mas que não é mais válida.

OBJETIVOS DA CRIPTOGRAFIA

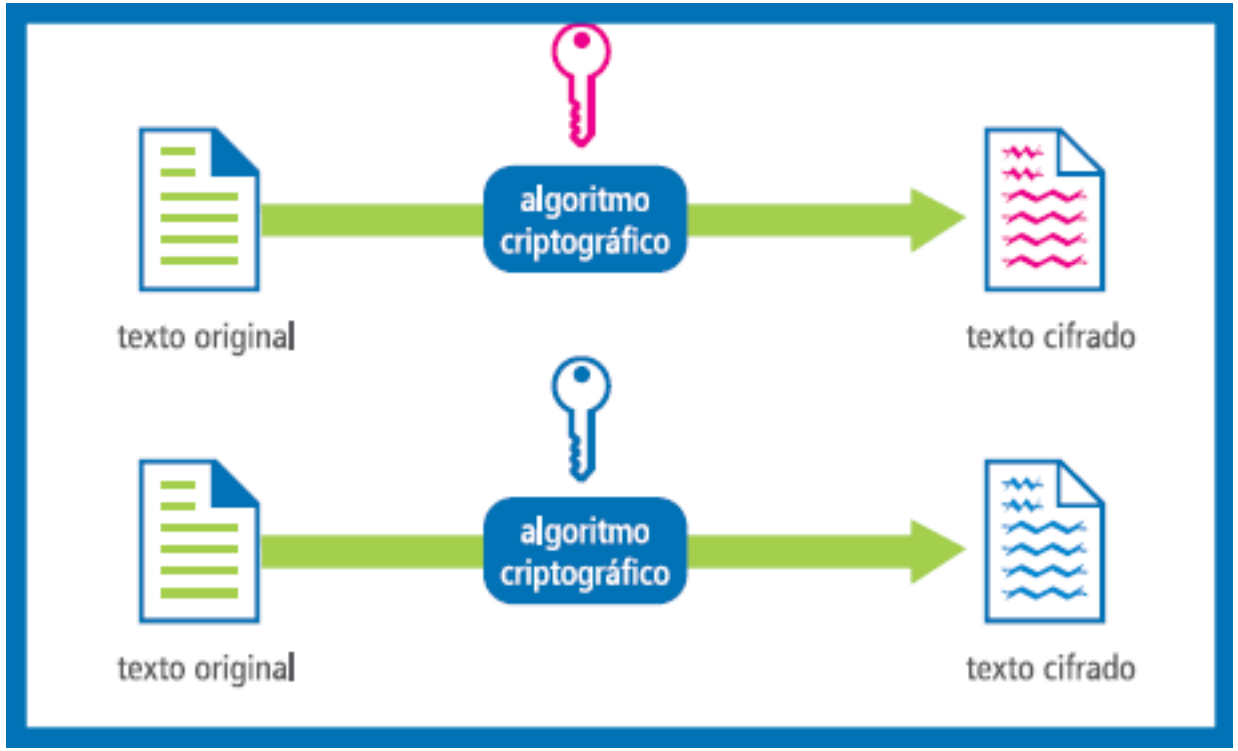
- **Autenticidade:** o destinatário verifica que a mensagem foi realmente enviada por quem diz ser enviada e é como a assinatura em um contrato ou em um cheque que pode ser reconhecida em cartório.
- **Irretratabilidade:** o remetente da mensagem não consegue negar a autoria da mensagem enviada. Isto ocorre porque uma vez publicada ou enviada a mensagem, o remetente não pode se retratar ou dizer que não enviou, já que somente ele tem o conhecimento ou a chave para gerar a mensagem.

PARA GARANTIR O FUNCIONAMENTO

- Os sistemas ou algoritmos de criptografia precisam cobrir todos esses princípios ao mesmo tempo e, na maioria das aplicações, é necessária a aplicação de mais um algoritmo em conjunto para atender a todos os requisitos.
- As técnicas mais conhecidas envolvem o **conceito de chaves**, as chamadas **chaves criptográficas**.

CHAVES CRIPTOGRÁFICAS

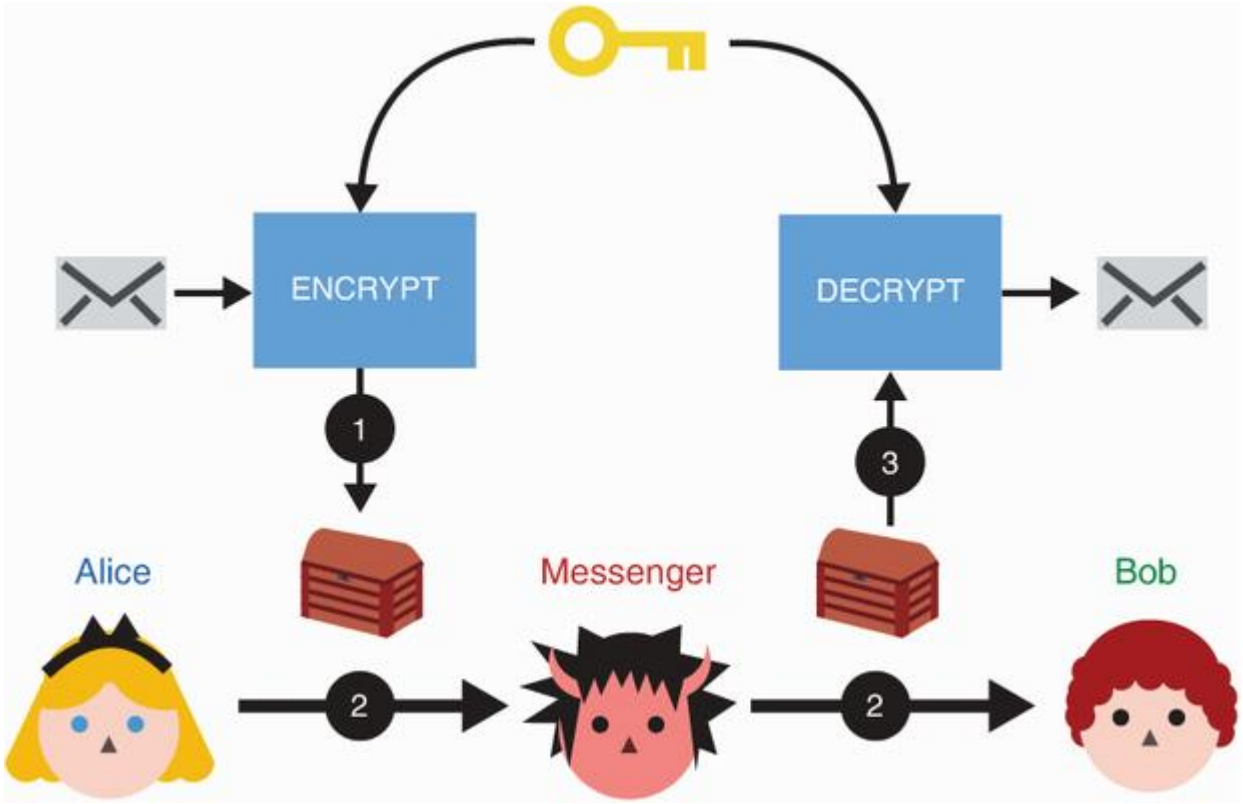
- São um conjunto de bits que trabalhando em conjunto com um **algoritmo de criptografia** é capaz de **codificar** e de **decodificar** informações.
- O **nível de segurança** da codificação depende tanto do **algoritmo** quanto do **tamanho da chave** escolhida (total de bits que ela possui).



FONTE: MACÊDO, 2011.

CRIPTOGRAFIA SIMÉTRICA

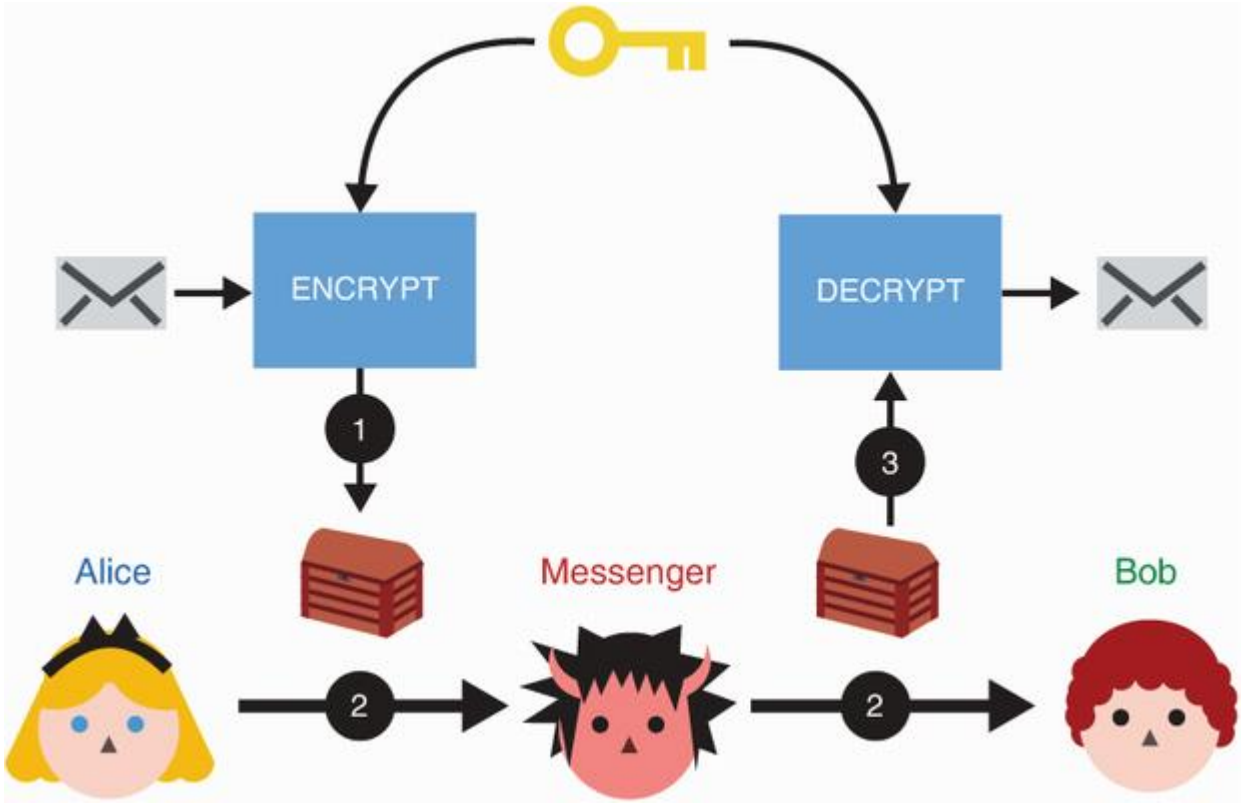
- **Criptografia Simétrica ou Criptografia de chave secreta** foi o primeiro tipo de criptografia criado onde os algoritmos que a utilizam têm como característica principal o uso **de uma mesma chave criptográfica** que criptografa ou descriptografa uma informação.



FONTE: WONG, 2021.

CRIPTOGRAFIA SIMÉTRICA

- No caso da criptografia digital, quanto mais bits forem utilizados, mais segura será a criptografia.
- Um algoritmo que use chaves de 8 bits, por exemplo, apenas 256 chaves poderão ser usadas na decodificação, pois 2 elevado a 8 é 256 e isto é inseguro, pois até uma pessoa é capaz de gerar as 256 combinações.



FONTE: WONG, 2021.

MODELOS DE ALGORITMO

- Para **chaves simétricas** oferece-se dois tipos de algoritmos:
  - **Cifras de blocos:** a mensagem é encriptada em blocos de tamanhos específicos.
  - **Cifra de fluxo ou *stream*:** a mensagem é encriptada pegando-se byte a byte da informação.
- Alguns algoritmos que utilizam esta técnica são o *Data Encryption Standard* **(DES)**, *Advanced Encryption Standard* **(AES)**, *Blowfish*, RC4, RC5, RC6 e etc.

CRIPTOGRAFIA ASSIMÉTRICA

- A **Criptografia Assimétrica ou de chave pública**, utiliza duas chaves diferentes no processo, **uma para encriptar e outra para decriptar.**
- Para **encriptar** utilizamos a **chave pública** e normalmente pode ser conhecida por qualquer pessoa.
- A chave usada para **decriptar** é a **chave privada** e é mantida em segredo por apenas uma das partes.

FONTE: MACÊDO, 2011.

CRIPTOGRAFIA ASSIMÉTRICA

- Esta técnica é utilizada para os princípios de **confidencialidade** e **autenticidade**.
- Um exemplo de sua aplicação é o uso do SSL utilizado no protocolo HTTPS com criptografia simétrica e assimétrica para criptografar e autenticar um website.
- RSA, *ElGamal* e *Diffie-Helman*, DSA e *Schnorr* são exemplos de algoritmos.

FONTE: MACÊDO, 2011.

ONDE CHEGAREMOS

- Conforme dissemos a criptografia deve apresentar os 4 princípios para ser considerada um recurso eficaz.
- Mesmo assim, ela não é capaz de garantir totalmente a segurança e o futuro é a técnica de **criptografia quântica.**
- Vamos ter que ficar atentos pois a **computação quântica** funcionará tanto para melhorar a criptografia quanto para quebrá-la.

REFERENCIAS BIBLIOGRÁFICAS

MACÊDO, Diego**.** Chaves Simétricas e Assimétricas, 2011. Disponível em: <https://www.diegomacedo.com.br/chaves-simetricas-assimetricas/>. Acesso em: 20 Set. 2022.

SILVA, Gabriel Leite Baptista da**.** Criptanálise. Disponível em: < https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/gabriel/hist.htm >. Acesso em 10 Set. 2022.

ALENCAR, Márcio Aurélio dos Santos. Fundamentos de redes de computadores / Márcio Aurélio dos Santos Alencar – Manaus : Universidade Federal do Amazonas, CETAM. 2010. Disponível em:<http://proedu.rnp.br/bitstream/handle/123456789/667/FundamentosRedesComputadores.pdf?sequence=2&isAllowed=y>.Acesso em: 27 Set. 2022.

REFERENCIAS BIBLIOGRÁFICAS

WONG, David. Real-World Cryptography. 1. ed. Manning Publications: Shelter Island, 2021. Disponível em:<https://learning.oreilly.com/library/view/real-world-cryptography/>. Acesso em: 6 Set. 2022.

JAMHOUR, E. Qualidade de serviços em redes IP. Curitiba: Programa de Pós-Graduação em Informática, Pontifícia Universidade Católica do Paraná, 2009. Disponível em:<https://www.ppgia.pucpr.br/~jamhour/Pessoal/Mestrado/TARC/QoSIP.pdf>. Acesso em: 6 mar. 2021.

DINAMIZE, 2022. O que é RFC e para que serve?. Disponível em:<https://www.dinamize.com.br/blog/o-que-e-rfc/>. Acesso em: 27 Set. 2021.


PUC Minas
Virtual