CRIPTOGRAFIA

DEFINIÇÃO DE CRIPTOGRAFIA

Segundo o site da Kaspersky: **Criptografia é a prática de codificar e decodificar dados.** Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica.

APLICAÇÃO DA CRIPTOGRAFIA

- Sites financeiros, do governo, de escolas e de compras costumam criptografar seus dados para ajudar na proteção contra roubo e fraude.

APLICAÇÃO DA CRIPTOGRAFIA

- **Proteção pessoal ou empresarial**:
- **Troca de informações**:
- **Criptomoedas**:
- **Certificado digital:**
- **Criptografia para e-mails**: **Criptografia de arquivo**:

Ferramentas de criptografia de arquivo

https://www.softdownload.com.br/10-programas-gratuitos-criptografar-arquivos-windows.html

CONCEITOS BÁSICOS DE CRIPTOGRAFIA DE DADOS

- converter a informação (cifrar) em outra (criptograma).

SEGREDO

- A segurança dos serviços criptográficos é baseada no segredo da chave criptográfica, que permite **cifrar** e **decifrar**, e não no método de transformar a informação, ou seja o algoritmo utilizado, que deve ser público.

TIPOS BÁSICOS DE ALGORITMOS CRIPTOGRAFIA

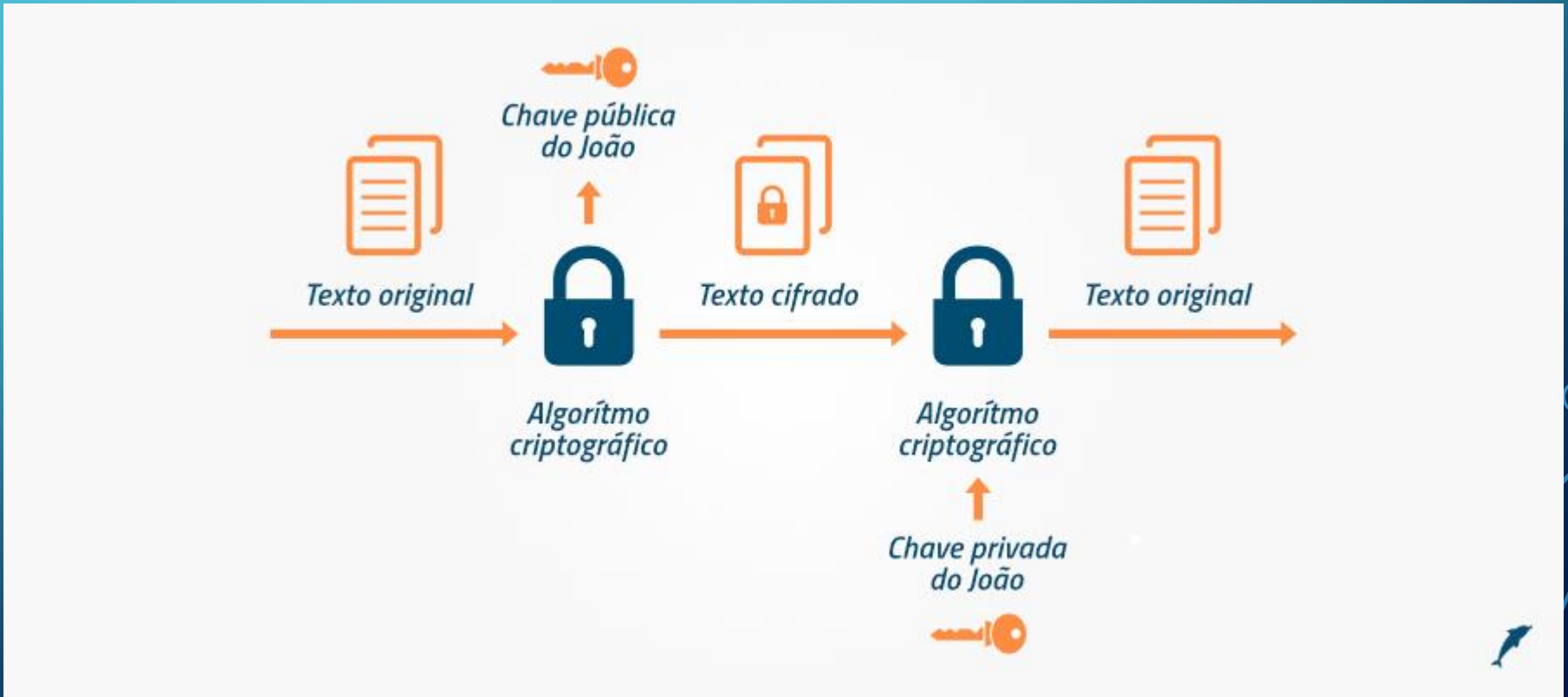
- **Chave simétricas**
- **Chaves assimétricas**

TIPOS BÁSICOS DE ALGORITMOS CRIPTOGRAFIA

- **Chave simétrica**

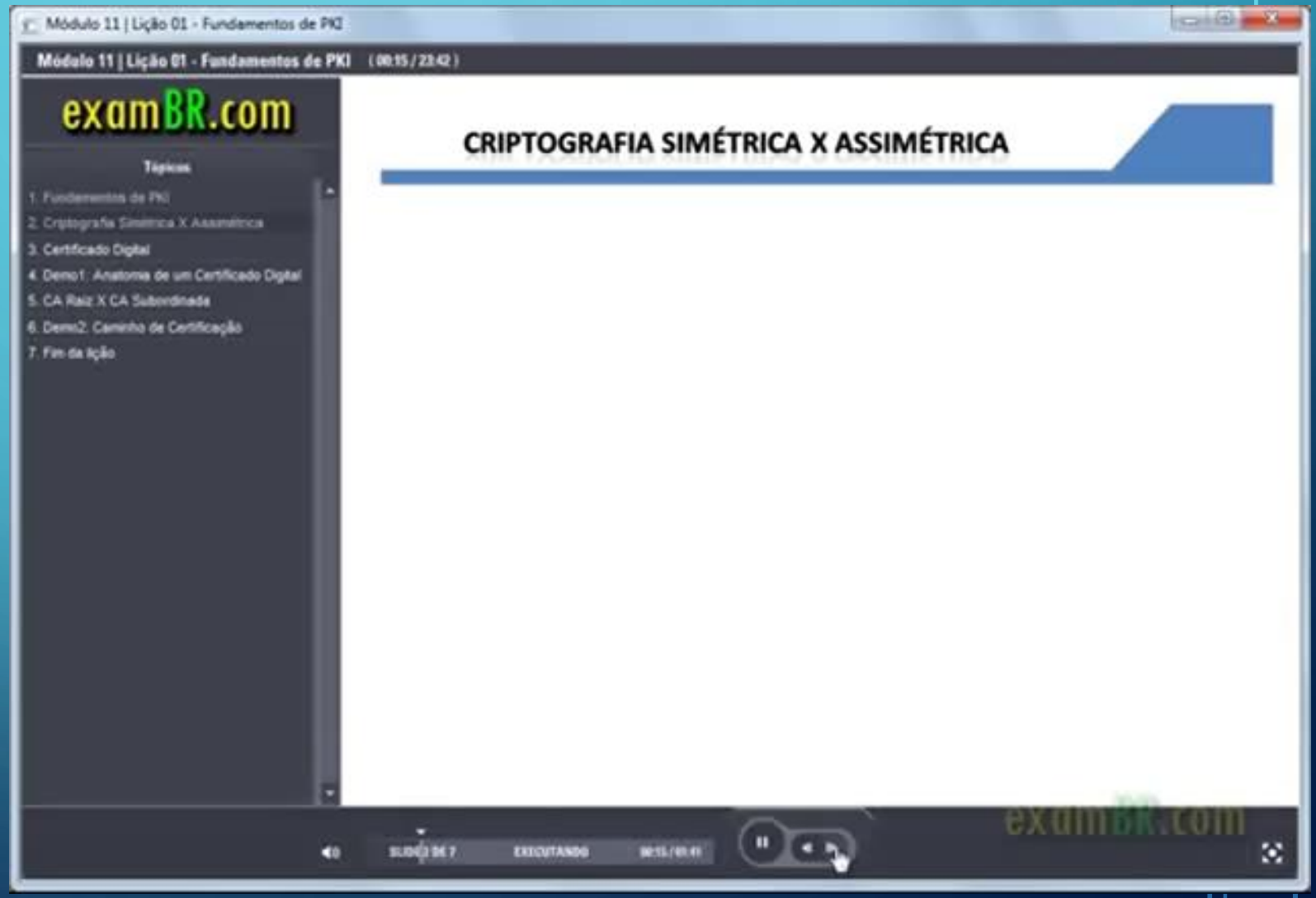
TIPOS BÁSICOS DE ALGORITMOS CRIPTOGRAFIA

- **Chaves assimétricas**



VEJAMOS UM VÍDEO.

- Link:
- https://www.youtube.com/watch?v=I3qEH3zIDr0

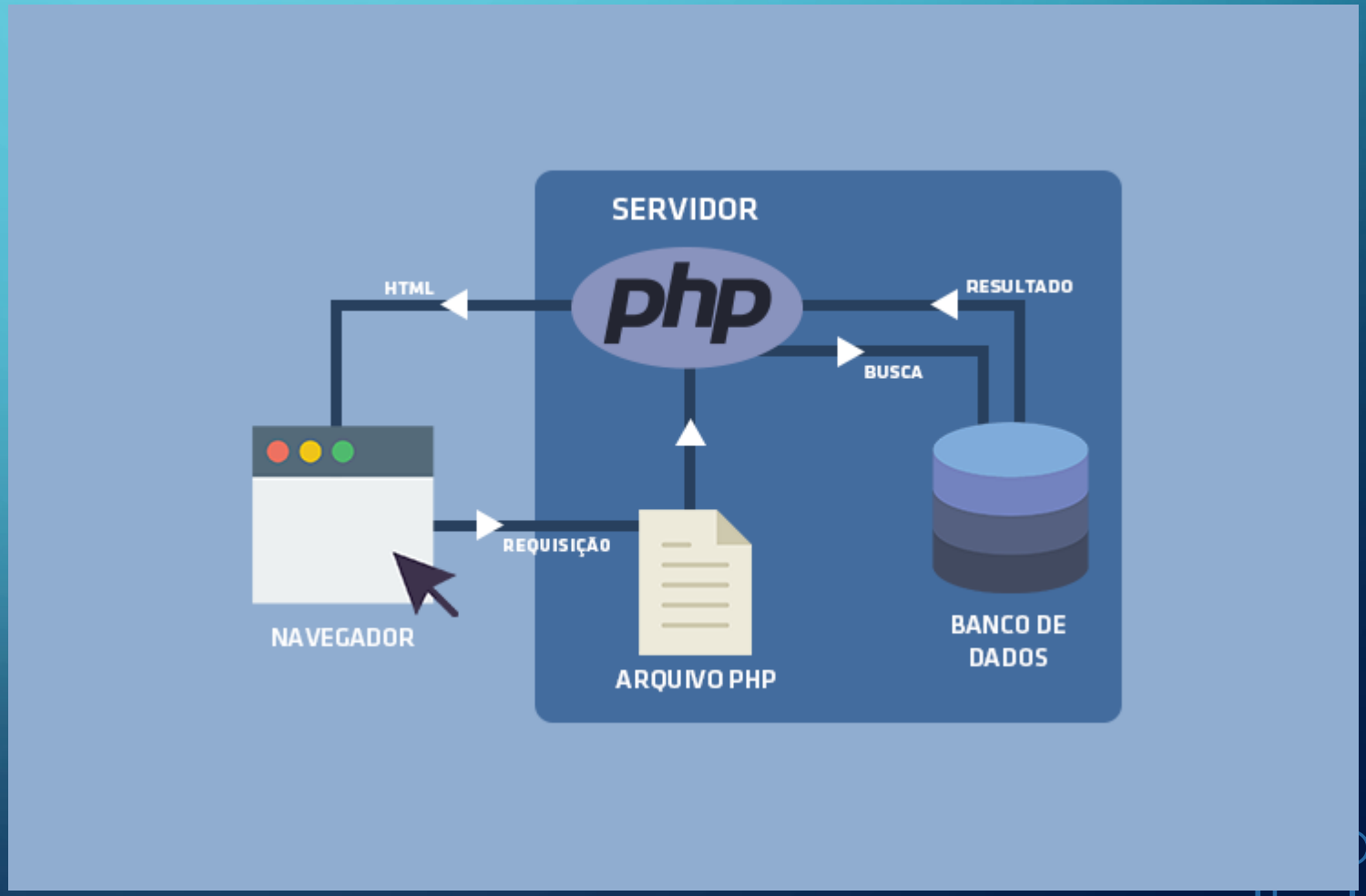


TIPOS DE CRIPTOGRAFIA MAIS USADAS

- **DES**
- *Data Encryption Standard* (DES)
  3DES
- O *Triple DES*
- **AES**
- *Advanced Encryption Standard* (AES) — ou *Padrão de Criptografia Avançada*
- **RSA**
- *Rivest-Shamir-Adleman* (RSA) foi um dos pioneiros em relação à criptografia de chave pública.

EXEMPLO

- criptografar uma senha:



FUNÇÃO HASH:

Função HASH:

É qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo.

•

FUNÇÃO HASH:

- ESTYA-6
- ZUNE-32
- MD2:
- MD4:
- MD5
- CRC32RIPEMD-160:
- SHA1
- SHA256:
- SHA512:

FUNÇÃO HASH:

Função HASH:

É qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo.

- Vamos usar uma função (algoritmo) para “criptografar” as senhas:

Senha:123456

Senha: %D11#m11*a2020

https://www.base64encode.org/

FUNÇÃO BASE 64:

Função HASH:

É qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo.

- Vamos usar uma função (algoritmo) para “criptografar” as senhas:

Senha:123456 MTIzNDU2

Senha: %D11#m11*a2020 JUQxMSNtMTEqYTIwMjA=

https://www.base64encode.org/

FUNÇÃO BASE 64:

Vamos decodificar

Senha: MTIzNDU2 123456

Senha: JUQxMSNtMTEqYTIwMjA= %D11#m11*a2020

https://www.base64encode.org/

FUNÇÃO MD5

Vamos codificar

Senha: 123456

Senha: %D11#m11*a2020

https://www.md5hashgenerator.com/

QUEBRAR HASH M5D

Vamos codificar

Senha: 123456

HASH MD5: e10adc3949ba59abbe56e057f20f883e

Senha: %D11#m11*a2020

HASH MD5: b809f56159b42da155ad12bd1f62288f

https://www.tiforense.com.br/identificador-de-hash/

https://crackstation.net/

https://hashes.com/en/decrypt/hash

FONTE:

- https://www.evaltec.com.br/criptografia-de-dados-e-gerenciamento-de-chaves/#:~:text=Em%20criptografia%20existem%20dois%20tipos,e%20a%20outra%20para%20decifrar
- https://cryptoid.com.br/valid/tipos-de-criptografia-conheca-os-10-mais-usados-e-como-funciona-cada-um/#:~:text=Criptografia%20Sim%C3%A9trica%20utiliza%20uma%20chave,por%20meio%20de%20um%20algoritmo
- Leia mais em: https://www.voitto.com.br/blog/artigo/o-que-e-hash-e-como-funciona

- https://base64.guru/converter/decode/image

- https://www.onlinehashcrack.com/

https://hashes.com/en/decrypt/hash

-