Introdução à Criptografia

Docentes: Dr. Sérgio Mavie, MSc., Dr. Justino Doho Eng

Eng. C. Maculuve

Maputo, 2023

Objectivos

- Definir criptografia;
- Descrever a história da criptografia;
- Identificar os objectivos da criptografia;
- Apresentar os conceitos básicos da criptografia;
- Apresentar os metemáticos da criptografia

Introdução à Criptografia

- A criptografia fornece níveis adicionais de segurança para os dados durante o processamento, armazenamento e comunicações;
- Ao longo dos anos, os matemáticos e cientistas da computação desenvolveram uma série de algoritmos cada vez mais complexos concebidos para assegurar confidencialidade, integridade, autenticação e não-repúdio.

Introdução à Criptografia

- Enquanto criptógrafos gastavam tempo desenvolvendo algoritmos de criptografia fortes, os atacantes gastavam seus importantes recursos para miná-los.

História de criptografia

- Desde o início da humanidade, os seres humanos criaram vários sistemas de comunicação por escrito, desde antigos hieróglifos escritos nas paredes das cavernas até aos CD / DVDs recheados com enciclopédias cheias de informações.
- A humanidade tem se comunicado usando meios secretos para esconder o verdadeiro significado dessas comunicações.

História de criptografia

- Por exemplo, sociedades antigas usavam um sistema complexo de símbolos secretos para representar lugares seguros para ficar durante os tempos de guerra.
- Civilizações modernas usam uma variedade de códigos e cifras para facilitar a comunicação privada entre indivíduos e grupos.
- Outro exemplo da aplicação da criptografia é a compra pela internet:

História de criptografia

- A informação que permite a transação – valor e descrição do produto adquirido – precisa estar disponível no dia e na hora que o cliente desejar efetuar (**Disponibilidade**).
- O valor da transação não pode ser alterado (**Integridade**).
- Somente o cliente que esta comprando e o comerciante devem ter acesso a transação (**Controlo de acesso**).

História de criptografia

- O cliente que esta comprando deve ser quem diz ser (**Autenticidade**).
- O cliente tem como provar o pagamento e o comerciante não tem como negar o recebimento (**Não - repúdio**).
- O conhecimento do processo da transação fica restrito aos envolvidos (**Confidencialidade**).

Cifra de César (*Caeser Cipher*)

- Um dos primeiros sistemas de cifra conhecido foi usado por Júlio César para se comunicar com Cícero, em Roma, enquanto ele estava conquistando a Europa.
- O sistema é extremamente simples: para criptografar uma mensagem, basta deslocar cada letra do alfabeto três casas para a direita.
- Por exemplo, A se tornaria D e B se tornaria E.

Cifra de César (Caeser Cipher)

- Se chegar ao fim do alfabeto durante este processo, basta só prolongar ao início de modo que X se torne A, Y torna-se B e Z se torna C.
- A cifra de César é uma cifra de substituição monoalfabética que é também conhecido como uma cifra C3 ou ROT3.

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Codificado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

História de Criptografia

- Em 1918, Arthur Scherbius desenvolveu uma máquina de criptografia chamada Enigma, utilizada amplamente pela marinha de guerra alemã em 1926.
- Durante a chamada "Guerra Fria", foram criados e utilizados diversos métodos a fim de esconder mensagens a respeito de estratégias e operações, criptografadas com diferentes métodos e chaves

Definição de Criptografia

- É a arte de escrever ou resolver códigos (“um sistema de sinais pré-arranjados, especialmente usado para garantir segurança na transmissão de mensagens") (The Concise Oxford Dictionary, 2006) – Criptografia clássica;
- É o estudo científico de técnicas para proteger informação digital, transacções e computação distribuída – criptografia moderna(Katz&Lindell,2008).

Definição de Criptografia

- Historicamente, os maiores consumidores de criptografia eram militares e organizações de inteligência.
- Hoje, todavia, a criptografia está em qualquer lugar;
- Mecanismos de segurança baseadas em criptografia são uma parte integral de quase todos sistemas de computadores.

Conceitos de Criptografia

- **Texto Plano** – é um arquivo qualquer (mensagem, texto, imagem, etc) que é conteúdo legível para todos. É sinónimo de texto aberto, texto claro ou texto legível.
- **Texto Cifrado** – Informação codificada ou por outra, é resultado de passagem de um texto plano por algum sistema criptográfico
- **Encriptação** – Processo de passagem de *plaintext* em cifra.
- **Decriptação** – Processo inverso à encriptação.

Conceitos de Criptografia

- **Chave** – Código usado pelos algoritmos para criptografar os dados. A chave pode ser secreta ou pública.
- **Criptografia** – Ciência ou arte que dispõe de mecanismos para transformar um texto plano em um texto cifrado e vice-versa.
- **Criptoanálise** - Ciência que estuda mecanismos para quebrar os textos cifrados, através de diversas técnicas e ferramentas de ataques a um sistema criptográfico.

Conceitos de Criptografia

Criptosistema – É uma quíntupla (M, C, K, E, D).

- **M** - representa mensagens não cifradas (*plaintext*);
- **C** - representa mensagens cifradas;
- **K** -representa as chaves empregues no criptosistema;
- **E** - transformações de criptografia que se aplicam a cada elemento de M para obter um elemento de C;
- **D** - o conjunto de transformações de decriptografia, análogo a E.

Conceitos de Criptografia

- Criptosistemas simétricos ou de Chave privada – aqueles que empregam a mesma chave K tanto para cifrar/criptografar quanto para decifrar/decriptografar.
- Inconveniente: a chave K deve ser partilhada pelo emissor e pelo receptor
- Como transmitir a chave de forma segura?

Conceitos de Criptografia

- Criptosistemas Assimétricos ou de Chave publica – empregam uma chave dupla (Kp – chave privada e Ku – chave publica)
- Inconveniente: tem um custo computacional muito maior que criptosistemas simétricos.
- Klong = 32, 64, 128, 256, 512, 1024 ou 2048 bits
- 2^ Klong combinações para decifrar a mensagem.

Exercício

1. Usando a cifra de César ROT3, decifra a seguinte mensagem: “F R Q J U D W X O D W L R Q V B R X J R W L W”
2. Usando a cifra de César ROT3, cifre “CRIPTOGRAFIA E SEGURANÇA DE DADOS”, ignorant espaços.
    1. ZOFMQLDOXCFXBPBDRXKZXABAXALP
    2. FULSWRJUDILD H VHJXUDQÇD GH GDGRV
    3. FULSWRJUDILD H VHJXUDQÇD GH GDGRV
    4. FULSWRJUDILD H VHJXUDQFD GH GDGRV

Obrigado