Segurança da Informação– GBC083

Prof. Rodrigo Sanches Miani – FACOM/UFU

Aula passada

Segurança da Informação– GBC083

Aula passada

- Confidencialidade, integridade e disponibilidade;
- Exemplos de ataques;
- Exemplos de mecanismos de defesas;
- Segurança em camadas;
  - Segurança envolve aspectos tecnológicos, técnicos, sociais, humanos e educacionais.

Princípios de Criptografia

Auditoria e Segurança da Informação– GSI035

Tópicos

1. Motivação
2. Definições
3. Exemplos
4. Breve histórico
5. Visão geral
6. Caracterização dos sistemas criptográficos

Motivação

Segurança da Informação– GBC083

Problema

Considere um sistema de comércio eletrônico. Em tal sistema, transações contendo dados sigilosos são realizadas entre duas entidades que, em geral, estão fisicamente distantes.

- Como os dados sigilosos são trafegados sem que terceiros não autorizados possam capturá-los?
- Como as entidades sabem que estão conversando entre si, ou seja, como elas podem criar um nível de confiança?

Problema

Considere um sistema de comércio eletrônico. Em tal sistema, transações contendo dados sigilosos são realizadas entre duas entidades que, em geral, estão fisicamente distantes.

- Como os dados sigilosos são trafegados sem que terceiros não autorizados possam capturá-los?
- Como as entidades sabem que estão conversando entre si, ou seja, como elas podem criar um nível de confiança?

Sistemas de **criptografia** são utilizados para resolver os problemas acima...

Definições

Segurança da Informação– GBC083

Criptografia – Definições básicas

- Def. 1 "Criptografia – é a ciência responsável por manter trocas de mensagens **seguras"**;

- Uma outra definição mais objetiva:
  - Def. 2 - *É o ato de alterar uma mensagem para esconder o significado desta.*
  - Como a alteração é feita? Algoritmos criptográficos!
  - Def. 2.1 – "Algoritmo criptográfico é uma função matemática utilizada para cifrar (esconder) e decifrar (revelar) um determinado dado"

Criptografia – Definições básicas

- Possui duas fases básicas:
  - Cifragem (*encryption*) – processo de disfarçar a mensagem original, também chamado de texto claro (*plaintext* ou *cleartext*);
  - Decifragem (*decryption*) – processo de transformar o texto cifrado (*ciphertext*) de volta em texto claro original.

- Os processos de cifragem e decifragem são realizados com auxílio de algoritmos que, muitas vezes, implementam diversas funções matemáticas.

Visão geral da criptografia

- Criptografia vem do grego e significa "escrita secreta".
- Não está ligada necessariamente à segurança de redes. É um conceito mais amplo e antigo.
- Historicamente, militares e diplomatas estão entre os que mais contribuíram para a criptografia.

Exemplos

Segurança da Informação– GBC083

Visão geral da criptografia – Exemplo simples

- Substituir cada letra na mensagem por uma letra três posições à frente.

```
texto em claro (P): meet me after the toga party
texto cifrado (C):  phhw ph dwihu wkh wrjd sduwb
```

- Substituição monoalfabética.

Visão geral da criptografia – Exemplo simples

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C

Esse algoritmo é seguro?

Visão geral da criptografia – Cifra de Vigenère

- Cifra de Vigenère – Múltiplas cifras de César (cifra polialfabética);

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

Visão geral da criptografia – Cifra de Vigenère

Exemplo:

- Cifrar a seguinte frase: ATACARBASESUL ("atacar base Sul");
- Usar a seguinte chave:“LIMAO”;
- ATACARBASESUL - LIMAOLIMAOLIM;
  - Coluna – texto em claro;
  - Linha – chave;
- Qual é o texto cifrado???

Visão geral da criptografia – Cifra de Vigenère

- Motivou o início dos estudos relacionados à criptoanálise (criptanálise);
  - ***Criptoanálise*** **-** é a arte de tentar descobrir o texto cifrado e/ou a lógica utilizada em sua cifragem;

- Cifras polialfabéticas são mais difíceis de quebrar por análise de frequência;

- Se a chave é curta e constantemente repetida palavras comuns tem uma grande chance de serem cifradas usando as mesmas letras da chave, levando à descoberta de padrões repetidos no texto.

Visão geral da criptografia – Outras cifras…

- Veremos que a criptografia evoluiu conforme os diferentes tipos de ataques que foram feitos contra os algoritmos;

- A área militar e, mais recentemente, as inúmeras aplicações disponíveis na Internet foram os principais catalisadores para a evolução da criptografia.

Breve histórico

Segurança da Informação– GBC083

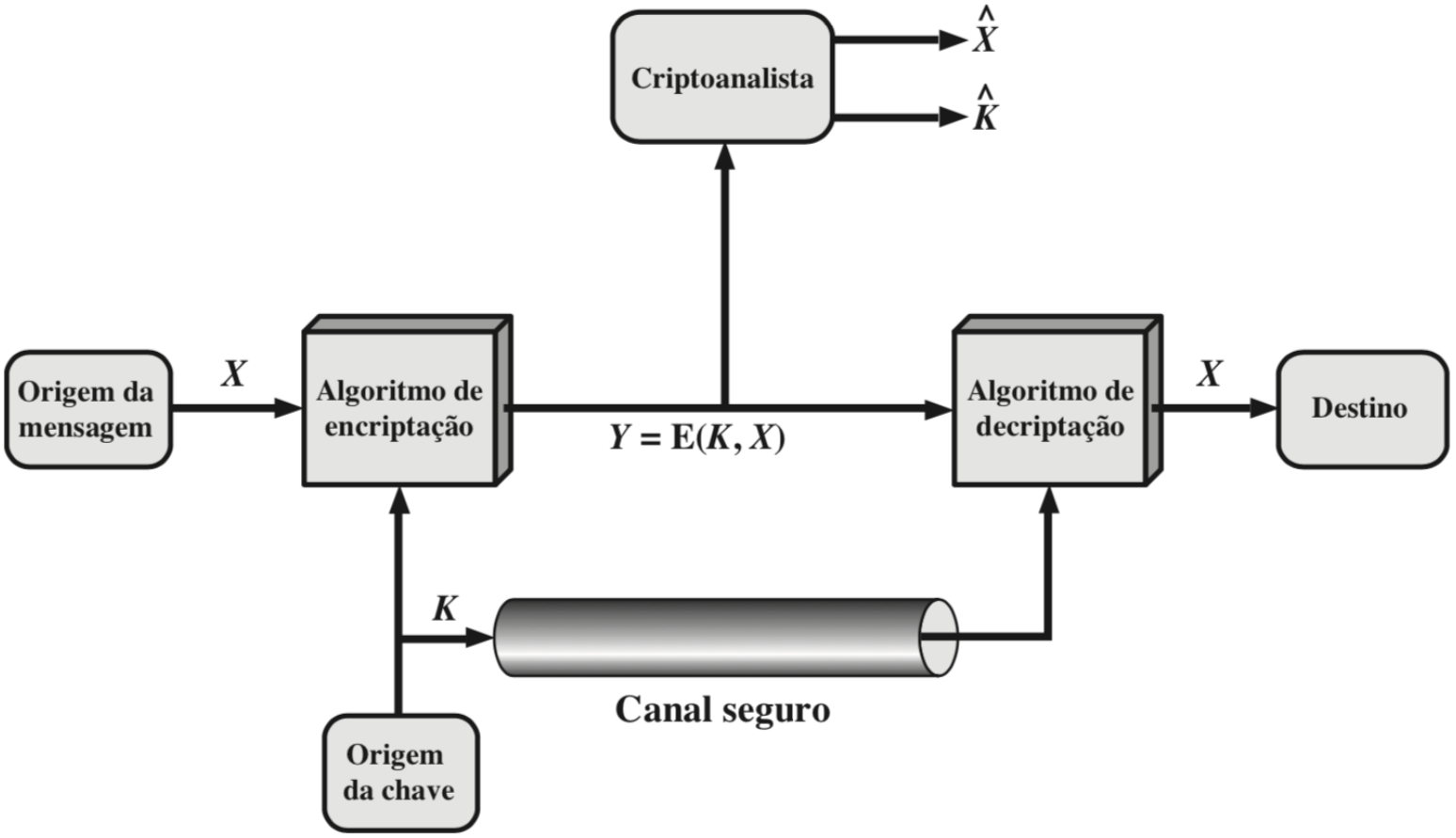
Criptografia – Breve histórico

- 1918 – Arthur Scherbius desenvolve Enigma, uma máquina de criptografia, utilizada pela marinha alemã;
- 1938 – Alan Turing inicia os estudos para quebrar as cifras geradas pela Enigma;
- 1948 – Teoria da Informação (Claude Shannon);
- 1970 – DES (Data Encryption Standard);
- 1976 – Diffie-Hellman;
- 1978 – RSA;
- 2002 – AES (Advanced Encryption Standard).
- "O livro dos códigos" – Simon Singh.

Visão geral

Segurança da Informação– GBC083

Visão geral da criptografia



Visão geral da criptografia

Pergunta: na opinião de vocês o algoritmo de criptografia pode ser público?

Visão geral da criptografia

Pergunta: na opinião de vocês o algoritmo de criptografia pode ser público?

E a chave?

Visão geral da criptografia

- Não podemos confiar a segurança com base no sigilo do método de criptografia.
- Esse método pode ser descoberto e a segurança acabará.
- A segurança está em cima da chave.
- A chave pode ser mudada facilmente caso seja quebrada. O método, muitas vezes, não.

Visão geral da criptografia

- A recomendação geral para a criptografia prevê um modelo genérico que todo mundo conheça.
- A segurança está no segredo da chave.
- Princípio de Kerckhoff (século XIX): todos os algoritmos são públicos; apenas as chaves são secretas.

Visão geral da criptografia

- Criptografia possibilita que as seguintes propriedades para a proteção da informação sejam alcançadas:
  - Sigilo (**confidencialidade**) – conteúdo ou existência da informação só será conhecido por pessoas autorizadas;
  - **Integridade** – Informação só pode ser alterada por pessoas autorizadas;
  - **Autenticidade** – Garante a identidade da origem do documento;
  - **Não-repúdio** (rejeição) – remetente e destinatário não podem negar que uma mensagem foi transmitida em um certo instante;

Caracterização dos sistemas criptográficos

Segurança da Informação– GBC083

Caracterização dos sistemas criptográficos

Três dimensões independentes:

1. Tipo das operações usadas para transformar o texto claro em texto cifrado;
2. Modo como o texto é processado;
3. Número de chaves usada.

Caracterização dos sistemas criptográficos

Tipo das operações usadas para transformar o texto claro em texto cifrado

- A maioria dos algoritmos de criptografia realizam dois tipos de operações:

1. **Substituição** – cada elemento do texto claro (bit, letra, grupo de bits ou letras) é mapeado em outro elemento;
2. **Transposição** – elementos no texto claro são reorganizados.

- Requisito fundamental é que nenhuma informação seja perdida – operações reversíveis!

Caracterização dos sistemas criptográficos

O modo como o texto claro é processado:

- Cifra de bloco
- Cifra de fluxo

Caracterização dos sistemas criptográficos

O modo como o texto claro é processado

- Uma **cifra de bloco** processa a entrada de um bloco de elementos de cada vez, produzindo um bloco de saída para cada bloco de entrada;
- Usadas em um cenário onde sabemos a quantidade de dados – arquivos, email, por exemplo. Bom para ser implementado em software.

Caracterização dos sistemas criptográficos

O modo como o texto claro é processado

- Um **cifra de fluxo** processa os elementos da entrada continuamente, produzindo a saída de um elemento de cada vez, enquanto prossegue (bit ou byte de cada vez);
- Aplicadas para situações onde há um fluxo de dados contínuo (não sabemos a quantidade de dados) como em um canal de comunicação. Bom para ser implementado em hardware.

Caracterização dos sistemas criptográficos

Número de chaves usada

- Se tanto o emissor quanto o receptor utilizarem a mesma chave, o sistema é considerado como *criptografia simétrica* (chave única, secreta ou convencional).
- Se emissor e receptor usarem chaves diferentes, o sistema é considerado de *criptografia assimétrica*.

Criptografia – Exemplos de aplicações

- Sites de compras – Informações protegidas pelo protocolo de segurança *Transport Layer Security* (TLS) que implementa algoritmos de criptografia;
- Bancos usam TLS + alguma criptografia adicional;
- Secure Shell (SSH) implementa diversos protocolos de criptografia;
- Redes sem-fio usam criptografia para proteção dos acessos e sigilo das informações (WPA1, WPA2);
- Redes privadas virtuais (VPN's) usam o IP Security (IPSec) para a proteção da comunicação entre organizações;

Próximas aulas

- Principais ataques aos sistemas criptográficos.
- Criptografia simétrica – técnicas clássicas.

Roteiro de Estudos

1. Leitura do Capítulo 2.1 – "Criptografia e segurança de redes. Princípios e práticas". William Stallings;
2. Estudo da vídeo-aula referente ao Tópico 2;
3. Resolução do TP-1.