Segurança da Informação– GBC083

Prof. Rodrigo Sanches Miani – FACOM/UFU

Criptografia simétrica – técnicas clássicas

Segurança da Informação– GBC083

Tópicos

- Técnicas clássicas:
  - Substituição
  - Transposição
  - Rotor
  - Esteganografia

Técnicas de substituição

Segurança da Informação– GBC083

Técnicas clássicas - substituição

Cifra de César

- O uso mais antigo que conhecemos de uma cifra de substituição, e o mais simples, foi feito por Júlio César;

```
claro: 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
cifra: 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
```

- Suponha que um texto cifrado com a cifra de César foi interceptado. Se o atacante souber que tal cifra foi utilizada um ataque de força bruta pode ocorrer?

Técnicas clássicas - substituição

CHAVE	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Técnicas clássicas - substituição

Cifra de César

- Quais são os problemas com a Cifra de César?

Técnicas clássicas - substituição

Cifra de César

- Quais são os problemas com a Cifra de César?
  - Existem apenas 25 chaves;
  - A linguagem do texto claro é conhecida e facilmente reconhecível;
  - Com uma boa quantidade de texto cifrado disponível, é possível usar a **frequência relativa** das letras do alfabeto... "a" deve aparecer mais, em seguida "e" e assim sucessivamente.

Técnicas clássicas - substituição

Cifra Playfair

- Motivação: aumentar o número de chaves!
- Ideia: trata os digramas (duas letras) no texto claro como unidades isoladas e as traduz para digramas de texto cifrado;
- O algoritmo Playfair é baseado no uso de uma matriz 5 × 5 de letras construídas usando uma **palavra-chave**.

Técnicas clássicas - substituição

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

1. Cada letra de texto claro em um par é substituída por aquela que esteja em sua própria linha e na coluna ocupada pela outra letra de texto claro;
2. Letras de texto claro repetidas que estão no mesmo par são separadas por uma de preenchimento;
3. Duas letras de texto claro que estejam na mesma linha e coluna são substituídas pela letra à direita e pela letra abaixo, respectivamente.

- http://rumkin.com/tools/cipher/playfair.php

Técnicas clássicas - substituição

- A cifra Playfair é um grande avanço em relação às cifras monoalfabéticas simples;
- 26x26 = 676 digramas ao invés de 26 letras!
- Foi considerada indecifrável por muito tempo;
- Foi utilizada durante as duas grandes guerras mundiais;
- Ainda deixa intacta uma boa parte da estrutura da linguagem do texto...

Técnicas clássicas - substituição

- As cifras polialfabéticas tentaram melhorar o cenário anterior...

- A ideia era usar diferentes substituições monoalfabéticas enquanto se prossegue pela mensagem de texto claro.

Cifra de Vigenère

	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

Exemplo:
Texto claro: ATACARBASESUL
Chave: LIMAOLIMAOLIM
Texto cifrado: LBMCOCJMSSDCX

Técnicas clássicas - substituição

Exemplo:

- Texto claro: ATA**C**A**R**BASES**U**L
- Chave: LIMAOLIMAOLIM
- Texto cifrado: LBM**C**O**C**JMSSD**C**X

- A letra cifrada "C" possui diferentes correspondentes no texto claro: "R", "U" e o próprio "C";
- Ou seja, alguns padrões de frequência são ocultados;
- Contudo, nem todo o conhecimento da estrutura do texto é perdido…

Técnicas clássicas - substituição

- Dependendo do tamanho do texto será possível encontrar sequências de texto cifrado iguais;
  - Se tais sequências estiverem distantes a uma distância que seja múltiplo do tamanho da chave elas gerarão textos claros iguais;
- Um criptoanalista pode usar essa informação para inferir o tamanho da chave, aplicar técnicas de frequência e fazer bons palpites sobre a chave;
- Ou seja, com o poder computacional disponível atualmente, tal sistema não é considerado **computacionalmente seguro**.

Técnicas clássicas – *One-time pad*

- Durante a Primeira Guerra, um official do exército norte-americano chamado Joseph Mauborgne, propôs uma cifra chamada de One-time pad (OTP);
- Teoricamente, tal cifra poderia ser considerada **incondicionalmente segura**;
- O oficial usou a ideia da cifra de Vigenère e também de um sistema criptográfico conhecido como cifra de Vernam;
- Em linhas gerais a ideia é a seguinte...

Técnicas clássicas – *One-time pad*

1. Usar uma chave **aleatória** tão grande quanto a mensagem;
2. A chave deve ser usada para cifrar e decifrar uma mensagem, e depois **descartada**;
3. Cada **nova** mensagem exige uma **nova** chave com o mesmo tamanho.

Dessa forma, o texto cifrado é uma saída aleatória que não possui nenhum relacionamento estatístico com o texto claro, ou seja, não existe um meio de quebrar a criptografia!

Técnicas clássicas – *One-time pad*

texto cifrado:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
chave:	*pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih*
texto claro:*	mr mustard with the candlestick in the hall
texto cifrado:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
chave:	*mfugpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt*
texto claro:**	miss scarlet with the knife in the library

Dado qualquer texto claro de mesmo tamanho do texto cifrado, existe uma chave que o produz. Portanto, se você fizesse uma busca exaustiva em todas as chaves possíveis, acabaria com muitos textos claros legíveis, sem saber o original! Como o criptonalista sairia dessa situação?

Técnicas clássicas – *One-time pad*

- A segurança do *one-time pad é* inteiramente decorrente da **aleatoriedade** da chave;

- Se o fluxo de caracteres que constitui a chave for verdadeiramente aleatório, então o de caracteres que constitui o texto cifrado também o será;

- Ou seja, achamos o sistema criptográfico perfeito!

- Será?!

Técnicas clássicas – *One-time pad*

Problemas práticos:

1. Como criar grandes quantidades (e qualidade!) de chaves aleatórias regularmente?

2. Como distribuir e proteger uma quantidade absurda de chaves?

- Tais problemas atestam a utilidade **limitada** de tal tipo de cifra.

Técnicas de transposição

Segurança da Informação– GBC083

Técnicas de transposição

- As técnicas anteriores envolvem a substituição de um símbolo de texto cifrado por um de texto claro;
- Uma espécie bem diferente de mapeamento é obtida realizando-se algum tipo de **permutação** nas letras do texto claro;
- Essa técnica é referenciada como uma cifra de transposição.

Técnicas de transposição

Algoritmo 1:

1. Escreva o texto claro como uma sequência de diagonais;
2. Reescreva o texto como uma sequência de linhas.

Ex: "*meet me after the toga party*"

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

MEMATRHTGPRYETEFETEOAAT

Técnicas de transposição

Algoritmo 2:

1. Escreva a mensagem (texto claro) em um retângulo, linha por linha;
2. Escreva a mensagem cifrada lendo a mensagem coluna por coluna, mas permutando a ordem delas;

```
Chave:          4 3 1 2 5 6 7
Texto claro:    a t t a c k p
                o s t p o n e
                d u n t i l t
                w o a m x y z
Texto cifrado:  TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Técnicas de transposição

Posso melhorar o algoritmo 2 cifrando novamente o texto gerado por tal algoritmo;

O resultado será uma disposição mais irregular do texto original mas ainda contendo as mesmas frequências de letra do texto claro original.

```
Chave:     4 3 1 2 5 6 7
Entrada:   t t n a a p t
           m t s u o a o
           d w c o i x k
           n l y p e t z
Saída:     NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

Máquinas de rotor

Segurança da Informação– GBC083

Máquinas de rotor

- Várias etapas de cifragem poderiam produzir um algoritmo de criptografia mais robusto;

- Essa é a ideia de uma classe de sistemas chamada de máquinas de rotor.

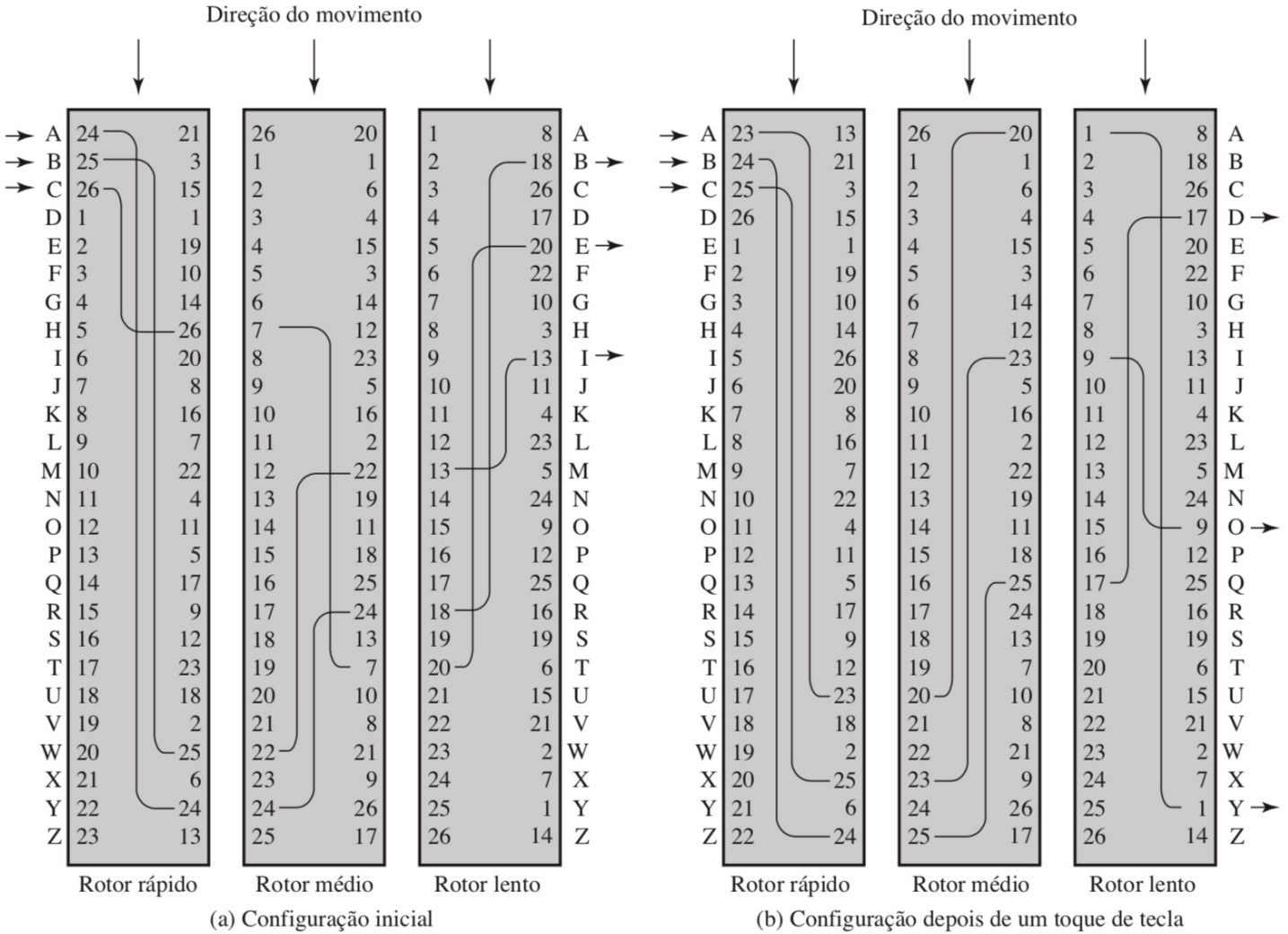
Máquinas de rotor

- A máquina consiste em um conjunto de cilindros rotativos independentes, através dos quais pulsos elétricos podem fluir;

- Cada cilindro tem 26 pinos de entrada e 26 pinos de saída, com fiação interna que conecta cada pino de entrada a um único pino de saída;

- Se associarmos cada pino de entrada e saída a uma letra do alfabeto, então um único cilindro define uma substituição monoalfabética.

Máquinas de rotor



Máquinas de rotor

- Para cada rotação completa do cilindro interno, o do meio gira uma posição de pino;
- Para cada rotação completa do cilindro do meio, o externo gira uma posição de pino;
- Quantos alfabetos de substituição existem para esse caso?

Máquinas de rotor

- Para cada rotação completa do cilindro interno, o do meio gira uma posição de pino;
- Para cada rotação completa do cilindro do meio, o externo gira uma posição de pino;
- Quantos alfabetos de substituição existem para esse caso?
  - 26x26x26 = 17576 alfabetos!
- O acréscimo de rotores aumenta o número de alfabetos de substituição diferentes...

Máquinas de rotor

- Um exemplo de máquina de rotor muito utilizada na prática foi a Enigma;

- O filme "O Jogo da Imitação" ilustra como Alan Turing e uma equipe de cientistas desvenda o protocolo criptográfico adotado pelos alemães (Máquina Enigma + Instruções de uso;

- O algoritmo simétrico DES, um dos mais utilizados comercialmente no mundo, foi fortemente baseado nas ideias das máquinas de rotores.

Esteganografia

Segurança da Informação– GBC083

Esteganografia

Uma mensagem em texto claro pode estar oculta de duas maneiras:

1. Os métodos de criptografia a tornam **ininteligível** a estranhos por meio de varias transformações do texto;
2. Os métodos de **esteganografia** escondem a **existência** da mensagem.

- Exemplo de esteganografia: um arranjo de palavras e letras em um texto aparentemente inofensivo forma a mensagem real.

Esteganografia

Embora essas técnicas pareçam arcaicas elas possuem aplicações modernas:

- Esconder uma mensagem usando os bits menos significativos dos frames em um arquivo de imagem;
  - Por exemplo, considere que cada pixel contém 24 bits de informação de cor RGB. O bit menos significativo de cada pixel de 24 bits pode ser alterado sem afetar muito a qualidade da imagem... Dependendo da qualidade de imagem, uma quantidade interessante de informação pode ser ocultada dessa forma.

Esteganografia

A figura abaixo possui uma mensagem oculta (também uma figura...)

Esteganografia

A figura abaixo possui uma mensagem oculta (também uma figura...)

- "*The hidden image is revealed by removing all but the two least significant bits of each color component and a subsequent normalization*." - Wikipedia

Esteganografia

- Costuma exigir muito *overhead* para esconder relativamente poucos bits de informação;
- Se o sistema for descoberto, se torna praticamente inútil;
- Porém, pode ser empregada como um meio alternativo sem a necessidade de chamar a atenção com o uso de criptografia.

Roteiro de Estudos

1. Leitura das seções 2.2, 2.3, 2.4 e 2.5 “Criptografia e segurança de redes. Princípios e práticas”. William Stallings;
2. Estudo das vídeo-aulas referentes ao Tópico 4;
3. Resolução do TP2.

Referências bibliográficas

- Stallings, W. Criptografia e segurança de redes: princípios e práticas. Pearson Prentice Hall, 2014.
  - **Capítulo 2**

- D. Boneh e V. Shoup, "A Graduate Course in Applied Cryptography", Online: https://crypto.stanford.edu/~dabo/cryptobook/
  - **Capítulos 2.1, 2.2 e 2.3**