Engenharia de Segurança

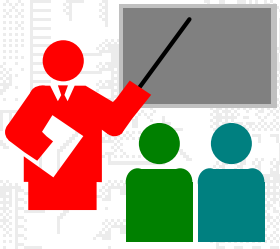
Profa. Dra. Kalinka Regina Lucas Jaquie Castelo Branco
kalinka@icmc.usp.br

Slides baseados nas transparências de diversos professores e autores de livros (prof. Edward David Moreno, Márcio H. C. d'Ávila, Tannenbaum, Kurose, Adriano Cansian entre outros)

Agenda - Criptografia

1. Serviços Criptográficos
2. Criptografia: Clássica e Moderna
3. Principais Algoritmos Simétricos

11/22/2010



2

Sistemas Criptográficos

- Técnicas que auxiliam a implementação dos serviços de segurança, principalmente:
  - Serviço de confidencialidade
  - Serviço de integridade
  - Serviço de autenticação
  - Serviço de irretratabilidade

3

Sistemas Criptográficos (2)

- Sistemas básicos
  - Algoritmos de criptografia
  - Algoritmos de troca de chaves
  - Funções *hash*
  - Algoritmos de particionamento de chaves

4

CRIPTOGRAFIA

Agenda

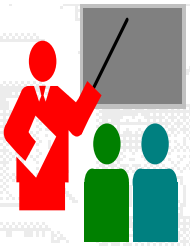
Introdução

Por que Criptografia ?

O que è criptografia ?

Como funciona a Criptografia ?

Classificação



Modelos de Sistemas de Criptografia

Modelo de Chave Convencional

Modelo de Chave Pública

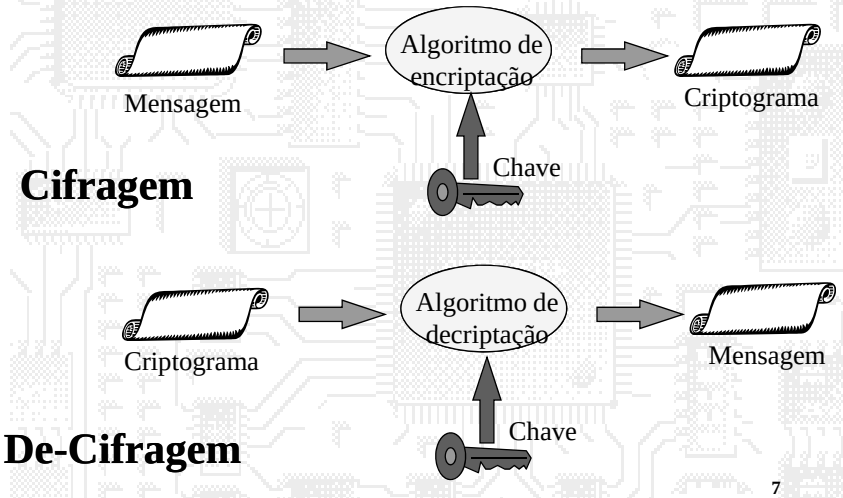
5

Criptografia - O que é ?

- **Processo de transformação**, através de uma chave secreta, de informação legível (mensagem) em informação ilegível (criptograma)
- Somente os indivíduos que conhecem a **chave secreta** tem capacidade de decifrar o criptograma e recriar a mensagem
- A dificuldade da decriptação reside em descobrir a chave secreta e não o segredo do método utilizado (algoritmo de criptografia).

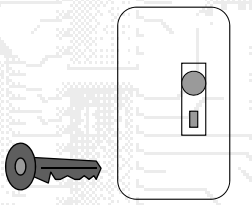
6

Criptografia - Como Funciona ?



7

Definições



Chave:

- Elemento que permite variar o processo de cifragem.
- Possibilita que cada entidade tenha um processo de codificação diferente da outra.
- Possibilidade de ocultar (“fechar”) uma determinada informação.
- As chaves são utilizadas para “guardar” informações e “recuperar” informações.

8

Definições (2)

Mensagem:

- Informação na **forma legível**
- Nos sistemas de computação é representada por uma **sequência de bits**.
- Exemplo:
  - Texto em portugûes, inglês, etc.
  - Programa fonte nalinguagem C
  - Programa fonte na linguagem Pascal
  - Programa executável
  - Imagem
  - Dados
  - Etc.

9

Definições (3)

Criptograma:

- Informação na **forma ilegível**
- Nos sistemas de computação é representada por uma **seqüência de bits**.

10

Criptografia - Classificação

- **Quanto ao tipo de operações de transformações**
  - **Substituição**
  - **Transposição**
- **Quanto ao Número de Chaves utilizadas**
  - **Simétrica**
  - **Assimétrica**
- **Quanto à forma de Processamento**
  - Por **bloco**
  - Por **stream** (fluxo)

11

Criptografia - Classificação

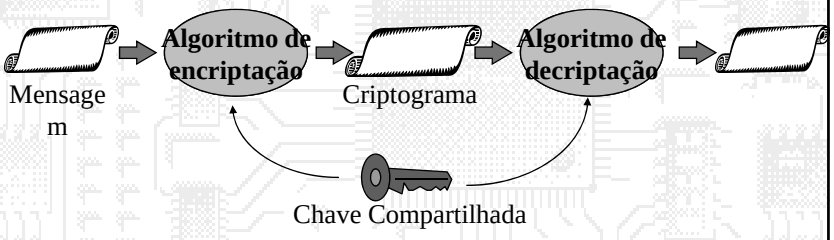
Quanto ao Número de Chaves

- Simétrica, convencional ou de chave privada
  - Quando o remetente e o destinatário da informação utilizam a mesma chave
- Assimétrica, de chave pública ou de chave dupla
  - Quando o remetente e o destinatário da informação utilizam chaves diferentes

12

Classificação - Simétrica (privada)

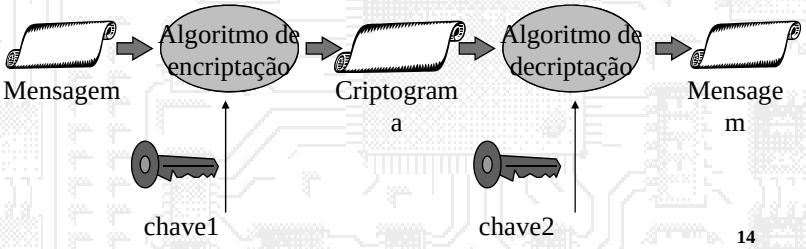
- **Criptografia Convencional**
  - Utiliza uma única chave
    - Os parceiros devem ter conhecimento da chave.
    - Ninguém mais deve conhece-la.



13

Classificação - Pública- Assimétrica

- **Criptografia de chave pública**
  - Utiliza duas chaves, normalmente
    - Uma privada: somente o dono a conhece
    - Uma pública: suposto que todos possam conhece-la



14

Criptografia - Classificação

Quanto à Forma de Processamento

- Por Bloco:
  - Processa um bloco de elementos por vez, produzindo assim um bloco de saída a cada vez.
- Stream:
  - Processa os elementos de entrada de forma contínua (bit a bit, ou byte a byte).

15

Criptografia - Classificação

Quanto ao Tipo de Operações

- Substituição:
  - Quando cada elemento do *plaintext* (bit, letra, grupo de bits, grupos de letras, etc.) é mapeado em um lemento no *ciphertext*.
- Transposição:
  - Quando os elementos do *plaintext* tem sua posição alterada no *ciphertext*.

16

Onde é útil a criptografia ?

- Na implementação de alguns serviços de segurança:
  - Confidencialidade:
    - Manter uma informação secreta
  - Autenticação
    - Autenticação de máquinas parceiras
    - Sistemas de autenticação de usuários baseados em chaves públicas
  - Integridade
    - Evitar alteração da informação de forma indevida
  - Irretratabilidade
    - Impede que o emissor da mensagem alegue que não tenha enviado ou que o receptor alegue que não tenha recebido.

Conclusão (Parcial)

17

Conclusão Parcial (2)

Onde a criptografia não ajuda ?

- Ataques destrutivos
- Informações não encriptadas
  - Antes da encriptação e/ou após a decriptação
- Senhas roubadas ou perdidas
- Traidores
- Criptoanálise realizada com sucesso

18

Conclusão Parcial (3)

O que é criptografia ?

- Processo de transformação, através de uma **chave secreta** de informação legível (*plaintext*) em informação ilegível (ciphertext).
- Somente os indivíduos que conhecem a chave podem decrifrar o *ciphertext* e criar novamente o *plaintext*.
- A dificuldade da decifragem reside em descobrir a chave secreta e não no segredo do método utilizado (algoritmo de criptografia).[19]

Conclusão Parcial (3)

Pergunta:

- Como a criptografia ajuda a implementar os serviços de segurança ?
- Veremos nos próximos módulos !

20

Exercícios

(1) Seja C o resultado da aplicação de um algoritmo de criptografia convencional sobre uma mensagem M utilizando-se uma chave K. O que é necessário para que uma entidade X possa decriptar esta mensagem ?

(2) Seja C o resultado da aplicação de um algoritmo de criptografia de chave pública sobre uma mensagem M utilizando-se uma chave K. O que é necessário para que uma entidade X possa decriptar esta mensagem?

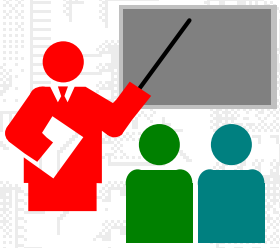
Exercícios (2)

(3) Sejam duas entidades A e B e CA o resultado da aplicação de um algoritmo de criptografia de chave pública sobre uma mensagem **MA** utilizando-se uma chave **KA** e **CB** o resultado sobre uma mensagem **MB** utilizando-se uma chave **KB**, cada uma com seu próprio par de chaves:

(a) CA pode ser decriptada com KA ?
(b) CA pode ser decriptada com KB ?
(c) CB pode ser decriptada com KB ?
(d) CB pode ser decriptada com KA ?
(e) O que é necessário para decriptar CA ?
(f) O que é necessário para decriptar CB ?

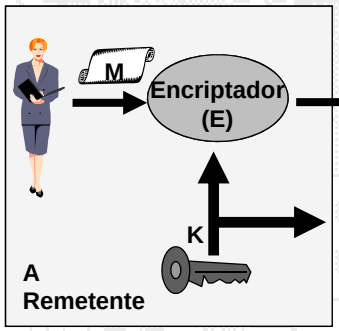
II. CRIPTOGRAFIA CONVENCIONAL

Técnicas Clássicas



23

CRIPTOGRAFIA CONVENCIONAL

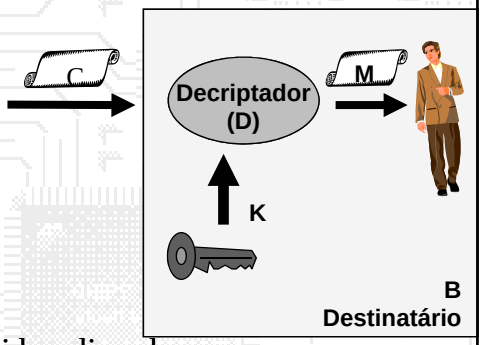


Encriptação:

* C = Ek(M)
* O Criptograma **C** é produzido aplicando uma função que é determinada utilização do algoritmo de encriptação **E** e pela chave **K** sobre a mensagem **M**

24

CRIPTOGRAFIA CONVENCIONAL



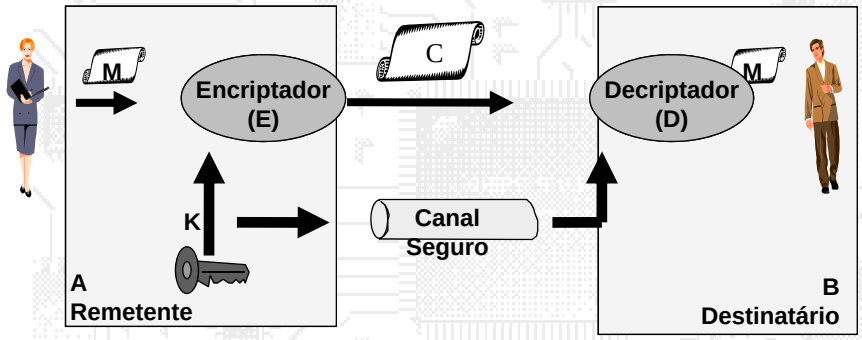
Decriptação:

* M = Dk(C)

* A mensagem **M** é produzida aplicando uma função que é determinada pela utilização do algoritmo de decriptação **D** e pela chave **K** sobre o ciphertext **C**.

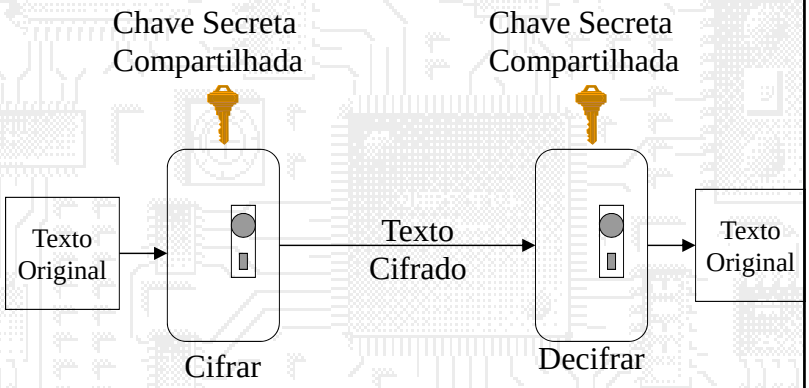
25

MODELO SIMPLIFICADO DA CRIPTOGRAFIA CONVENCIONAL



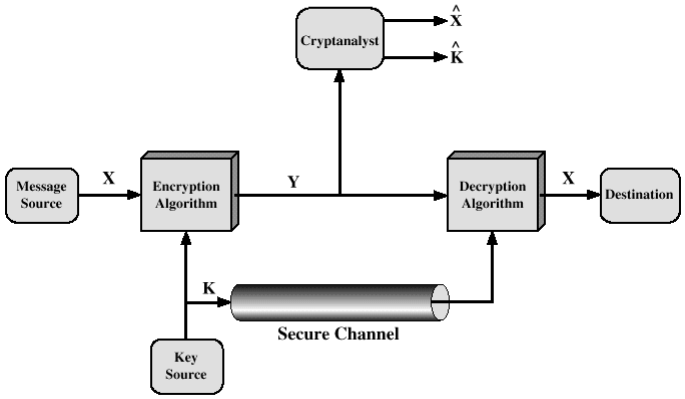
26

MODELO SIMPLIFICADO DA CRIPTOGRAFIA CONVENCIONAL



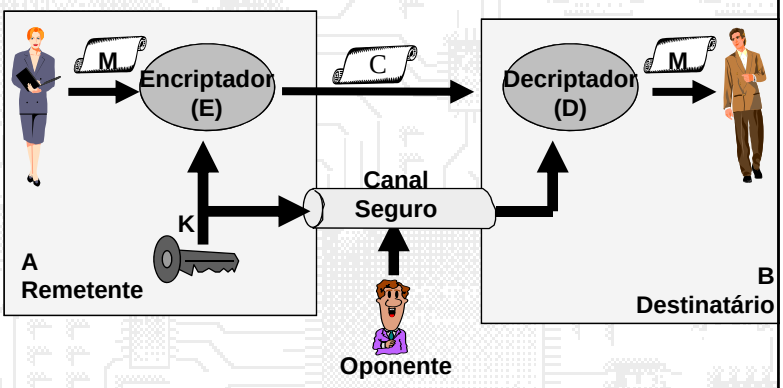
27

MODELO DE UM CRIPTOSISTEMA CONVENCIONAL



3

Problemas na CC



- Manter a chave secreta
- Distribuição da chave: necessita canal seguro !

Criptoanálise

- **Criptoanálise:**
  - "Ciência que abrange os princípios, métodos e meios para se chegar à decriptação de um criptograma".
- **Possíveis Objetivos:**
  - Decifrar um criptograma específico
    - Se o oponente estiver interessado em somente nesta mensagem específica
  - Decifrar a chave (K)
    - Se o oponente estiver interessado em decifrar várias mensagens.

30

CRIPTOANÁLISE

- **Força do Algoritmo de Criptografia**
  - A Criptografia convencional se baseia no presuposto que seja impraticável decrifrar uma mensagem conhecendo somente o criptograma e o algoritmo.

TEMPO MÉDIO DE BUSCA EXAUSTIVA

Tamanho da Chave	Número de Chaves	Tempo Requerido (1 cripto/µs)	Tempo Requerido (10^6 cripto/µs)
32	$2^{32} = 4{,}3x10^9$	35,8 minutos	2,15 milisegundos
56	$2^{56} = 7{,}2x10^{16}$	1.142 anos	10,01 horas
128	$2^{128} = 3{,}4x10^{38}$	$5{,}4x10^{24}$ anos	$5{,}4x10^{18}$ anos
26 Caracteres (permutação)	$26! = 4x10^{26}$	$6{,}4x10^{12}$ anos	$6{,}4x10^6$ anos

CUSTO COMPUTACIONAL PARA QUEBRA

	Tamanho da Chave (bits)					
Custo U$	40	56	64	80	112	128
100 K	2s	35 h	1 ano	70000 ano	10 e 14	10 e 19
1 M	200 ms	3,5 h	37 dias	7000 anos	10 e 13	10 e 18
10M	20s	21 m	4 dias	700 anos	10 e 12	10 e 17
100M	2 ms	2m	9 h	70 anos	10 e 11	10 e 16
1G	200 us	13 s	1 h	7 anos	10 e 10	10 e 15
10G	20 us	1 s	5,4 m	245 anos	10 e 9	10 e 14
100G	2 us	100 ms	32 s	24 anos	10 e 8	10 e 13
1T	0,2 us	10 ms	3 s	2,4 anos	10 e 7	10 e 12
10T	0,02 us	1 ms	300 ms	6 horas	10 e 6	10 e 11

Bruce Schneier, 1996

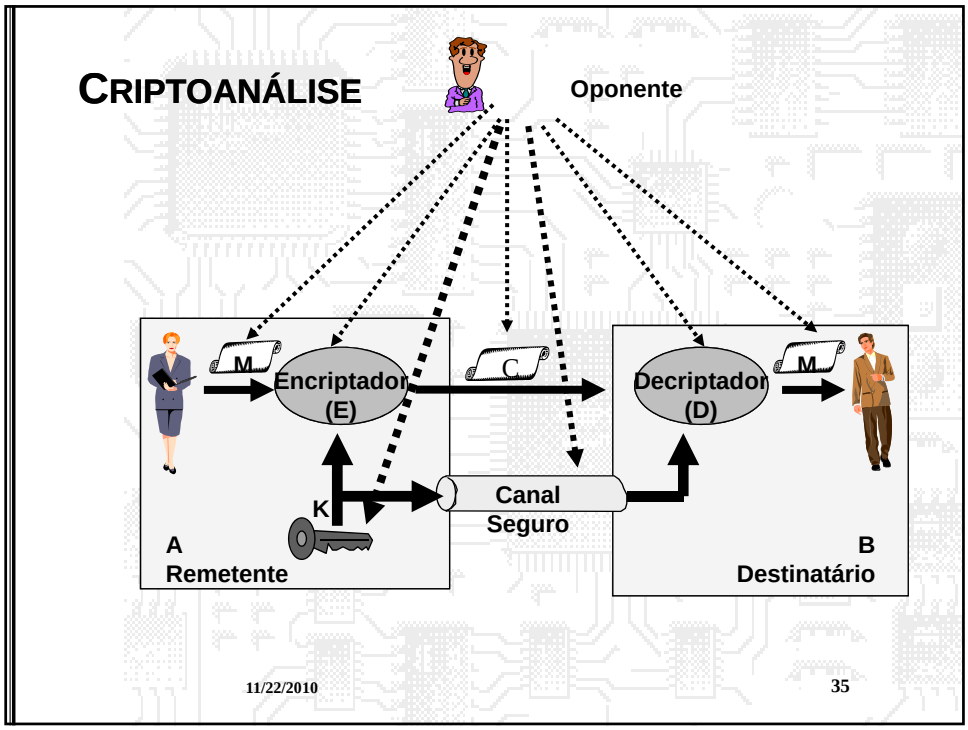
- **O poder computacional dobra a cada 1,5 anos**
- **Obs. Tempo de duração do universo = 10 e 10.**

Criptoanálise

Sempre é possível
decifrar uma mensagem !

Basta testar todas as chaves possíveis.
É somente uma questão de tempo!

Mas pode demorar mais que
o tempo de duração do universo!



Criptoanálise - Custos

- Custo computacional para quebra
  - Poder computacional dobra a cada 1,5 ano
  - Obs: Tempo de duração do universo = 10^{10} anos

2000	Tamanho da chave					
CustoU$	40 bits	56 bits	64 bits	80 bits	112 bits	128 bits
10 K	2 s	35 h	1 ano	70.000 anos	10^{14} anos	10^{19} anos
100 k	200 ms	3,5 h	37 dias	7.000 anos	10^{13} anos	10^{18} anos
1 M	20 s	21 m	4 dias	700 anos	10^{12} anos	10^{17} anos
10 M	2 ms	2 m	9 h	70 anos	10^{11} anos	10^{16} anos
100 M	200 us	13 s	1 h	7 anos	10^{10} anos	10^{15} anos
1 G	20 us	1 s	5,4 m	245 anos	10^{9} anos	10^{14} anos
10 G	2 us	100 ms	32 s	24 anos	10^{8} anos	10^{13} anos
100 G	0,2 us	10 ms	3 s	2,4 anos	10^{7} anos	10^{12} anos
1 T	.02 us	1 ms	300 ms	6 horas	10^{6} anos	10^{11} anos

36

Criptoanálise - Oponente

- Pode explorar vulnerabilidades do algoritmo
  - Necessita de conhecimentos de criptoanálise
- Pode estar a procura de pares mensagem-criptograma
  - Para tentar realizar ataque com força bruta
  - Para gerar livro código
- Pode tentar obter a chave no momento que é repassada para a entidade parceira
- Pode possuir um enorme poder computacional

37

Criptoanálise - Exemplo

- Suponha um sistema onde as informações sejam criptografadas por um algoritmo qualquer. Um usuário mantém em um determinado diretório os seguintes arquivos:
  - arq1.crypt - arq3.crypt
  - arq2.crypt - arq1.txt
- O arquivo arq1.txt não possue mensagem confidencial, portanto está aberto.
- Pergunta:
  - **Existe algum problema ?**

38

Criptoanálise - Exemplo

Existe a possibilidade de um oponente decifrar um criptograma (C) ou descobrir a chave (K) se:

- Vulnerabilidade do algoritmo
  - Os algoritmos de encriptação e decriptação forem vulneráveis
- Poder computacional
  - Possuir um enorme poder computacional
- Acesso à chave
  - **Conseguir acesso ao valor da chave (K)**

39

Criptoanálise - Força da Criptografia

- **Incondicionalmente segura**
  - Não importa quanto do criptograma esteja disponível, não é possível inferir a mensagem original.
  - Somente ONE-TIME-PAD são incondicionalmente seguros
- **Computacionalmente inviável (forte)**
  - O custo para a quebra deve ser muito maior que o valor da informação
  - A demora da quebra deve ser muito maior que o tempo de vida útil da informação (**OBS:** Levar em conta a evolução do poder computacional)

40

TIPOS DE ATAQUE

Tipo de Ataque	Conhecimento do Criptoanalista
Somente Texto Cifrado	• Algoritmo de Criptografia • Texto Cifrado
Texto Plano Conhecido	• Algoritmo de Criptografia • Texto Cifrado • Um ou mais pares de texto plano-cifrado
Texto Plano Escolhido	• Algoritmo de Criptografia • Texto Cifrado • Escolha do texto plano
Texto Cifrado Escolhido	• Algoritmo de Criptografia • Texto Cifrado • Escolha do texto cifrado
Texto Escolhido	• Algoritmo de Criptografia • Texto Cifrado • Escolha do texto plano • Escolha do texto cifrado

41

TIPOS DE ATAQUE

(1) Somente Criptograma

- O criptoanalista possui como informação para decifrar um criptograma somente o próprio criptograma.
- Pode também ter conhecimento da ocorrência de um determinado padrão na mensagem
  - Exemplo: Arquivos Postscript sempre iniciam com “%!PS”
- Lembre-se que o algoritmo sempre é conhecido.

42

TIPOS DE ATAQUE

(2) Mensagem Conhecida

- O criptoanalista possui pares mensagem-criptograma.

43

TIPOS DE ATAQUE

(3) Mensagem Escolhida

- O criptoanalista possui pares mensagem-criptograma
- Porém, foi o próprio criptoanalista quem criou as mensagens, possivelmente com determinados padrões
- Estas mensagens escolhidas foram submetidas ao encriptador (utilizando a chave K que não é de seu conhecimento) gerando assim o correspondente criptograma

44

TIPOS DE ATAQUE

(4) Ciphertext Escolhido

- O criptoanalista possui pares mensagem-criptograma
- Porém, neste caso, o criptoanalista foi quem criou o criptograma, possivelmente com determinados padrões
- Este criptograma escolhido foi submetido ao decriptador (utilizando a chave K que não é de seu conhecimento) gerando assim a correspondente mensagem.

45

TIPOS DE ATAQUE

(5) Mensagem e Criptograma Escolhido

- O criptoanalista possui dois pares mensagem-criptograma
- Um par mensagem-criptograma cujo plaintext criado foi submetido ao encriptador gerando o criptograma associado
- Um par mensagem-criptograma cujo criptograma criado foi submetido ao decriptador gerando a mensagem associada

46

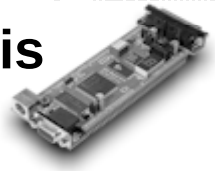
Principais Algoritmos

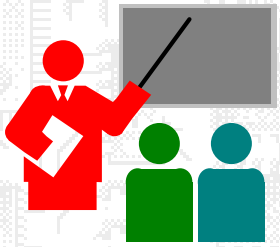
Nome	Tipo	Tam. chave	Tam. bloco
DES	bloco	56	64
Triple DES (2 ch.)	bloco	112	64
Triple DES (3 ch.)	bloco	168	64
IDEA	bloco	128	64
BLOWFISH	bloco	32 a 448	64
RC5	bloco	0 a 2040	32,64,128
CAST-128	bloco	40 a 128	64
RC2	bloco	0 a 1024	64
RC4	**stream**	**0 a 256**	**--**
Rijndael (AES)	bloco	128,192,256	128, 192, 256
MARS	bloco	variável	128
RC6	bloco	variável	128
Serpent	bloco	variável	128
Twofish	bloco	128,192,256	128

47

II. CRIPTOGRAFIA CONVENCIONAL

Algoritmos Posicionais





48

ALGORITMOS CLÁSSICOS

- **Baseados em Transposição:** Na qual as letras do plaintext são trocadas de posição
- **Baseados em Substituição:**
  - Na qual as letras do plaintext são substituídas por outras letras, números ou símbolos
  - Se o plaintext for visto como uma seqüência de bits, então a substituição envolve a substituição de padrões de blocos de bits do plaintext por outro padrão de blocos de bits no ciphertext.

49

ALGORITMOS CLÁSSICOS

- **Baseados em Transposição:**
  - Transposição de colunas
- **Baseados em Substituição:**
  - Cifra de César
  - Cifra Monoalfabética
  - Substituição Homofônica
  - Playfair
  - Cifra de Vigerère
  - Cifra de Vigerère com autochave
  - Máquina de rotação

50

TÉCNICAS CLÁSSICAS
CIFRADOR DE CÉSAR

```
Plano:   meet me after the toga party
cifrado: PHHW PH DIWHU WKH WRJD SDUWB
```

```
Plano:   abcdefghijklmnopqrstuvwxyz
cifrado: DEFGHIJKLMNOPQRSTUVWXYZABC
```

Encriptar	*Decriptar*
C=E(p)=(p+3) mod 26	p=D(p)=(C-k) mod 26
C=E(p)=(p+k) mod 26	

51

CIFRADORES MONOALFABÉTICOS

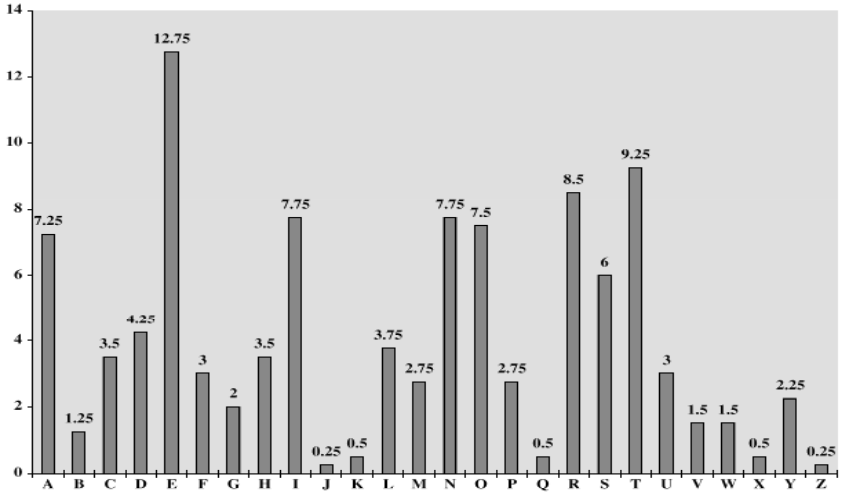
- Qualquer permutação de 26 caracteres alfanuméricos
- 26! = 4×10^{26} possíveis chaves

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHDMZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

P 13,33	H 5,83	F 3,33	B 1,67	C 0,00
Z 11,67	D 5,00	W 3,33	G 1,67	K 0,00
S 8,33	E 5,00	Q 2,50	Y 1,67	L 0,00
U 8,33	V 4,17	T 2,50	I 0,83	N 0,00
O 7,50	X 4,17	A 1,67	J 0,83	R 0,00
M 6,67				

52

FREQÜÊNCIA RELATIVA DAS LETRAS NA LÍNGUA INGLESA



CRIPTOANÁLISE

- ***P*** e ***Z*** são equivalentes a ***e*** e ***t***
- ***S, U, O, M*** e ***H*** -> {***r,n,i,o,a,s***}
- ***A, B, G, Y, I*** e ***J*** -> {***w,v,b,k,x,q,j,z***}
- Digramas, Trigramas
  - ***th*** é o mais comum -> ***ZW***
  - ***P -> e*** (***ZWP*** -> ***the***)
- ***ZWSZ -> th_t*** ***S->a*** ***That***

54

CRIPTOANÁLISE

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHDMZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

Criptoanálise

It was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

55

CIFRADOR PLAYFAIR

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

2 em 2 letras

Letras repetidas usa-se caracter preenchedor. Ex: x
Letras na mesma linha trocadas pela seguinte
Letras na mesma coluna trocadas pela seguinte
Para o restante, usa-se a coluna do outro

```
departamento de informática
CKSODZROGMPR CK AGPHMOSRBEB
```

56

CIFRADORES POLIALFABÉTICOS

Vigenère - **Auto Chave**
Vernam - xor

Joseph Mauborgne - **one-time pad**

$$C_i = p_i \oplus k_i$$
$$p_i = C_i \oplus k_i$$

	a	b	c	..	z
a	A	B	C		Z
b	B	C	D		A
c	C	D	E		B
:					
z	Z	A			Y

Exemplo:

```
deceptivedeceptivedeceptive
wearediscoveredsaveyourself
ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

57

TÉCNICAS DE TRANSPOSIÇÃO - 1

troqueascaixasapossinomeiodia

t o u a c i a a o s n m i d a
r q e s a x s p s i o e o i

touaciaaosnmidarqesaxspsioeoi

58

TÉCNICAS DE TRANSPOSIÇÃO - 2

Chave: 4 3 1 2 5 6 7
Texto Plano: p e g u e a c
a i x a a z u
l a d a p e l
a m a n h a q
Texto Cifrado: GXDAUAANEIAMPALAEAPHAZEACULQ

59

ANÁLISE DA TRANSPOSIÇÃO

4	3	1	2	5	6	7
p	e	g	u	e	a	c
a	i	x	a	a	z	u
l	a	d	a	p	e	l
a	m	a	n	h	a	q

↓

4	3	1	2	5	6	7
g	x	d	a	u	a	a
n	e	i	a	m	p	a
l	a	e	a	p	h	a
z	e	a	c	u	l	q

Pegue a caixa azulada pela manha q

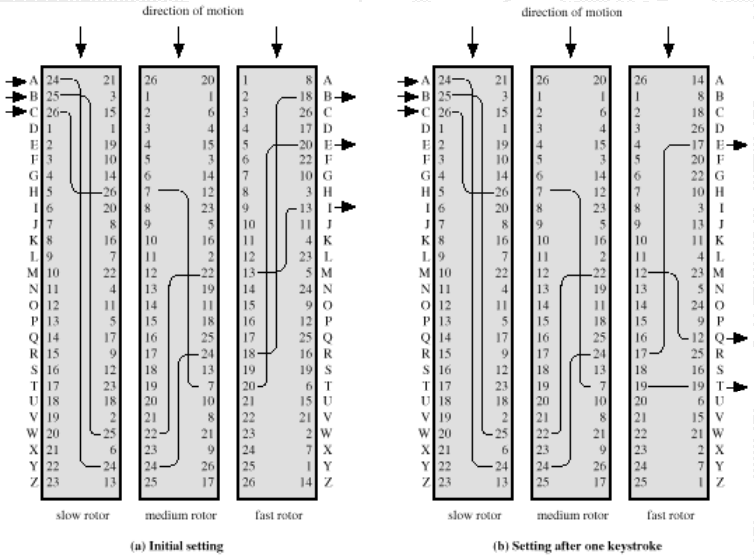
01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28

03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28

17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28

60

ENIGMA - MÁQUINA DE TRÊS ROTORES



MÁQUINA DE ROTAÇÃO

- Criptoanálise
  - Nchaves = $26^3 = 17576$
    - (p/3 cilindros distintos)
  - N domínio = 26
  - Ataques:
    - (1) Ciphertext somente: Força bruta
    - (2) Plaintext Conhecido: ?
    - (3) Plaintext selecionado: Direto, exemplo:
      - Plaintext: “aaaaaaaaaaa ..a”, (26^N vezes p/ N cilindros)
    - (4) Ciphertext Escolhido
      - Direto, exemplo:
        - Ciphertext: “aaaaaaaaaa ... ‘” (26^N vezes p/ N cilindros)

62

EXERCÍCIOS

- (1) Criptografe o plaintext “exercício” utilizando os algoritmos e chaves apresentadas
- (2) Dentre os algoritmos **posicionais** quais podem ser descobertos de forma direta pelo ataque com “plaintext Escolhido” onde é utilizada a seguinte mensagem:
  - “abcdefghijklmnopqrstuvwxyz”

63

EXERCÍCIOS (2)

- (3) Dentre os algoritmos vistos quais podem ser descobertos de forma direta pelo ataque com “Plaintext Escolhido” onde é utilizada a seguinte mensagem:
  - “aaaaaaaaaaaaaaaaaaaaa...”; \
- (4) Dentre os algoritmos vistos quais podem ser descobertos de forma direta pelo ataque “Plaintext Conhecido’.
- (5) A facilidade ao ataque pela força bruta também está relacionado ao número de chaves possíveis no algoritmo. Qual o número de chaves possíveis de cada um dos algoritmos apresentados ?

64