Criptografia Aplicada

Jean Everson Martina

Nota sobre a autoria

- Material por Jean Everson Martina
- Adição de conteúdo
  - Dayana Spagnuelo
  - Lucas Perin

Cryptography and Network Security

Principles and Practice (second editiond)

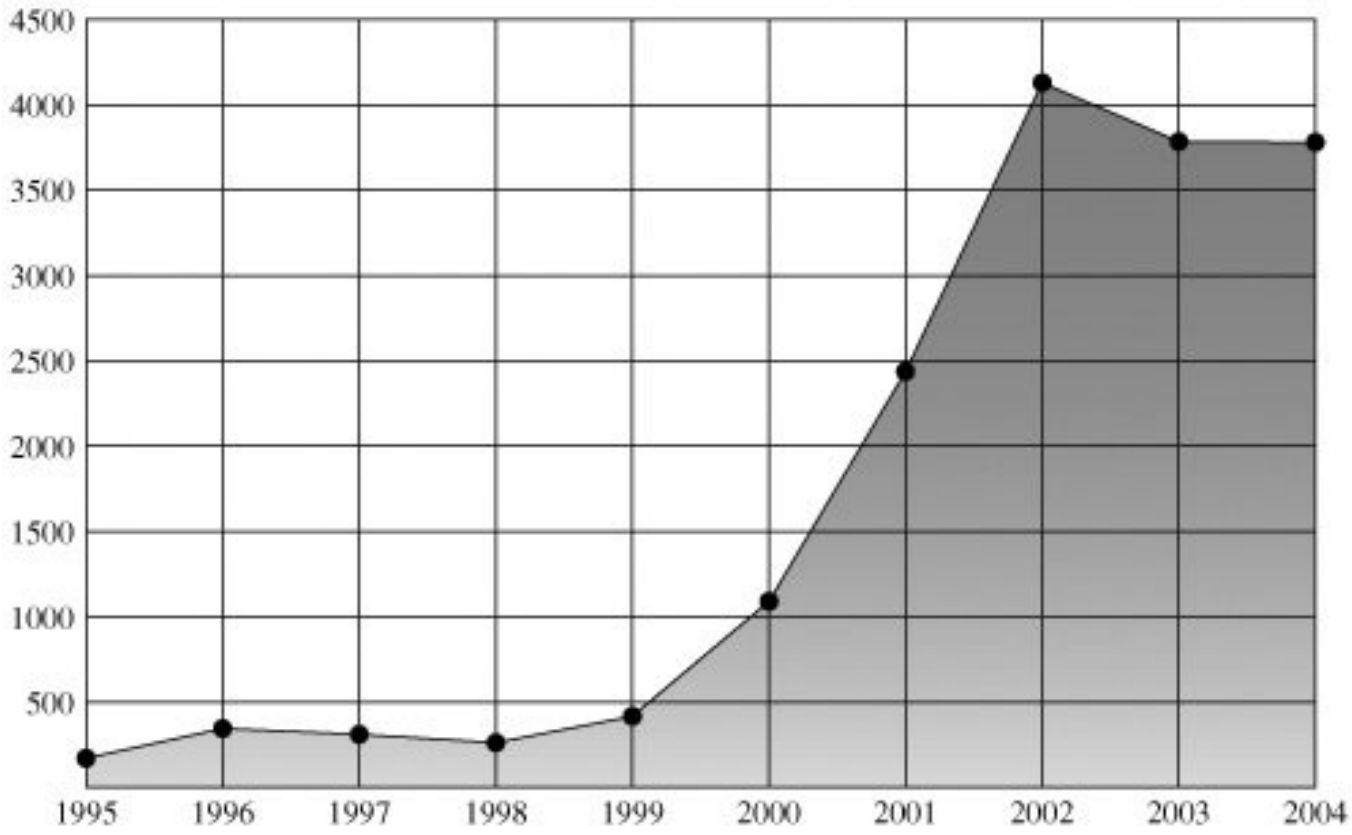
William Stallings

Por que estudar segurança?

- RFC 1636 (Security in the internet architecture) lançado em 1994
  - Constatava que a internet precisava de mais segurança
  - Proteção de infra estrutura de rede
  - Monitoramento e controle de tráfego
  - Segurança user-end-user (autenticação e cifras)

"On the Internet, nobody knows you're a dog."

Tendências em (In)Segurança

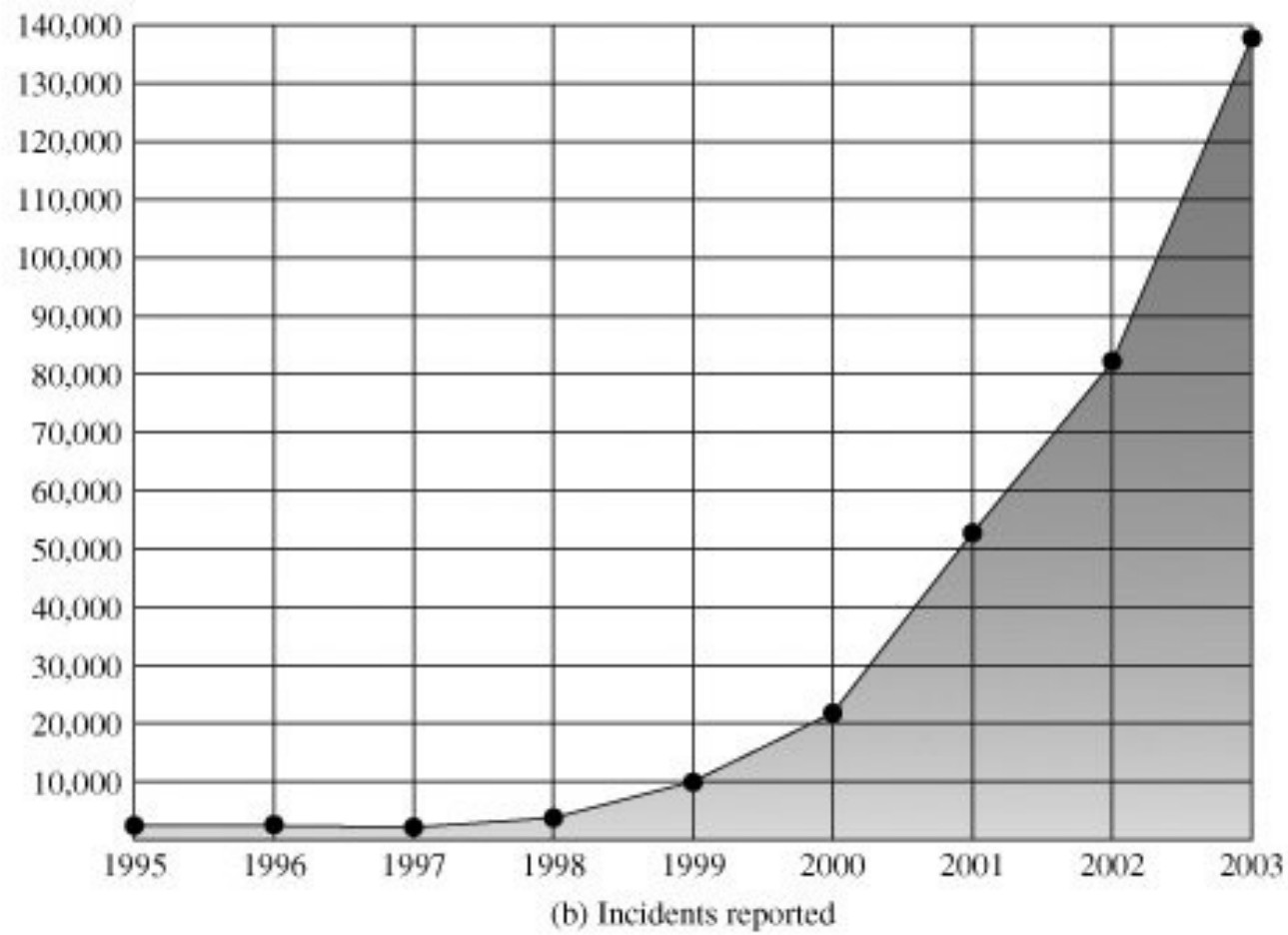


(a) Vulnerabilities reported

Tendências em (In)Segurança

- Rede
- Aplicação
- Sistemas Operacionais
- Roteadores

Tendências em (In)Segurança

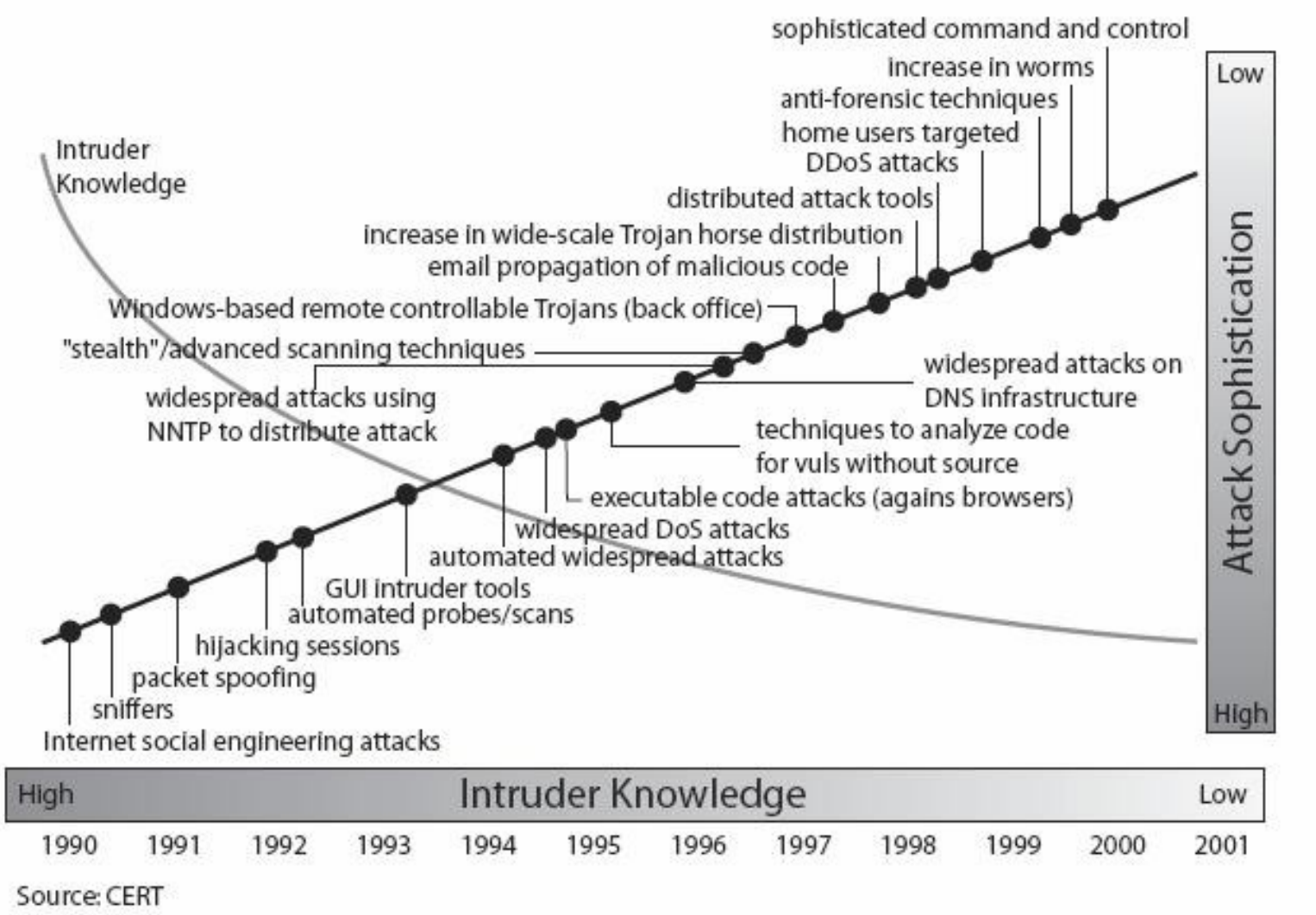


(b) Incidents reported

Tendências em (In)Segurança

- Negação de serviço (DoS)
- IP Spoofing - pacotes com IP falso para explorar aplicativos que usam identificação a partir do IP
- Escuta de pacotes

Tendências em (In)Segurança



Arquitetura de Segurança OSI

- Recomendação lançada em meados de 1991
- Área de segurança precisava de mais organização
- Modelo sistemático
  - Definir requisitos de segurança
  - Cumprir os requisitos definidos
  - Escolha de mecanismos e políticas de segurança
- Definiu conceitos utilizados até hoje

Arquitetura de Segurança OSI

- Ameaça:
  - Potencial de violação
  - Vulnerabilidade
  - Brecha de segurança
- Ataque:
  - Investida em uma ameaça
  - Ação que compromete a segurança
  - Tentativa deliberada de explorar uma brecha

Arquitetura de Segurança OSI

- Mecanismo de Segurança:
  - Processo ou dispositivo
  - Detectar, prevenir, ou recuperar ataques
- Serviços de Segurança:
  - Aumenta a segurança dos dados
  - Processo ou serviço
  - Contra ataques
  - 1 ou mais mecanismos de segurança

Ataques Passivos

Ataques passivos tem objetivo de obter/ler informações do sistema sem afetar os recursos do mesmo.

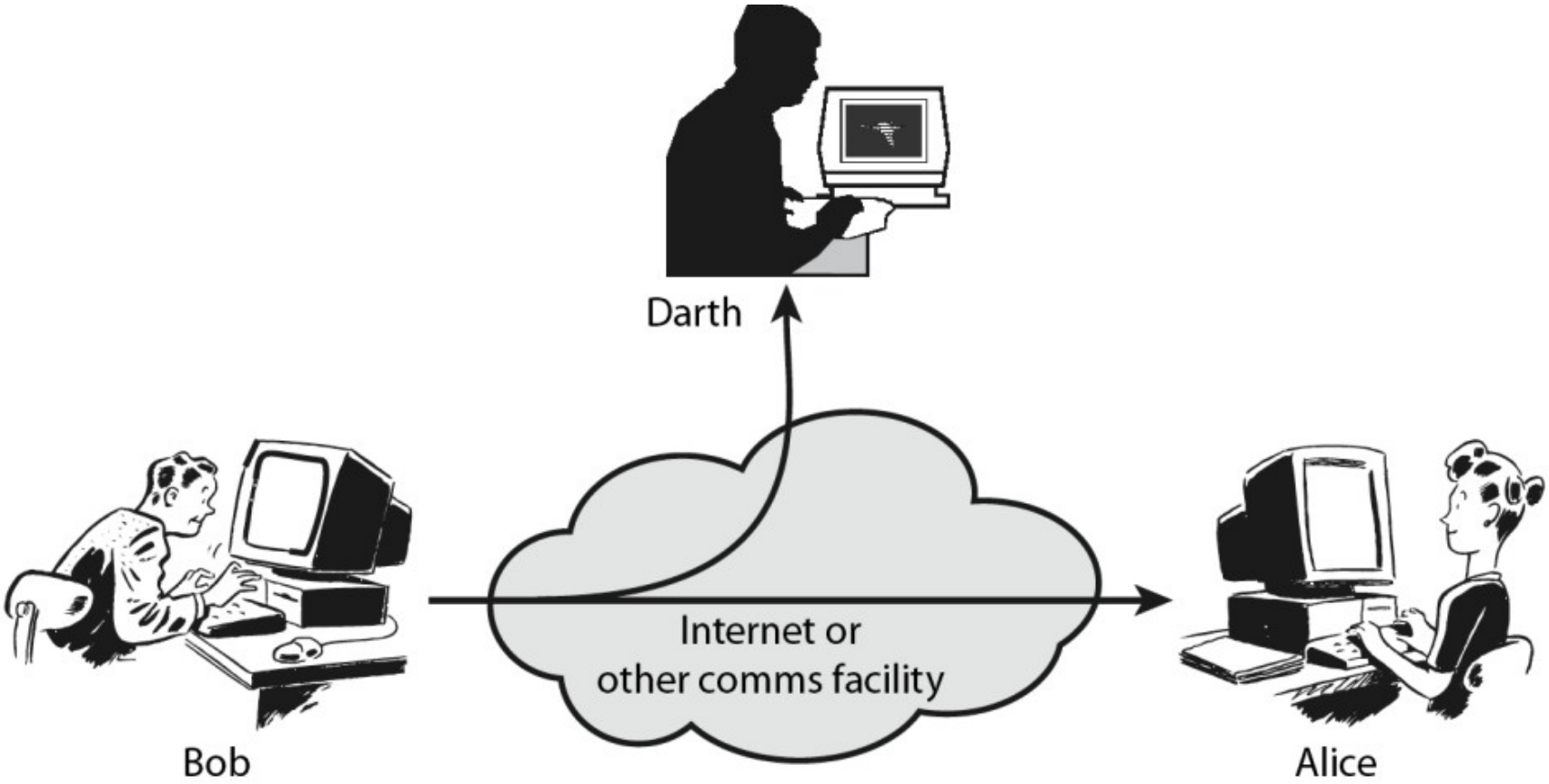
Ataques Passivos

- Vazamento de Informação:
  - Engenharia Social
  - Descuido
- Analise de Trafego:
  - Inferência para obter a informação
  - Análise de freqüência e tamanho de mensagens

Ataques Passivos

Ataques passivos são difíceis de detectar porque não alteram os dados

Ataques Passivos



Ataques Ativos

- Mascaramento
  - A acredita que C é B
  - Impersonating
- Repetição
  - Re-uso de informação trocada por A e B
- Modificação de Mensagens
  - Alteração do conteúdo da mensagem entre A e B
- Negação de Serviços
  - Prevenção da comunicação entre A e B

Ataques Ativos x Passivos

- Ataques passivos são difíceis de detectar, mas fáceis de previnir
- Ataques ativos são fáceis de detectar, mas difíceis de previnir
  - Se aproveitam de vulnerabilidades muitas vezes não conhecidas
  - Defesas focam em detectar e recuperar, ao invés de previnir

Serviços de Segurança (RFC 2828)

- De acordo com a RFC 2828:

"Um serviço provido por um sistema para prover determinado tipo de proteção ao recursos do sistema; ***serviços de segurança implementam políticas de segurança e são implementados por mecanismos de segurança.***"

Serviços de Segurança (RFC 2828)

- Autenticação
  - Autenticação da contra-parte
  - Autenticação dos dados (garantia da fonte)
- Controle de Acesso
- Confidencialidade
- Integridade
- Não Repudio (Origem e Destino)
- Disponibilidade

Mecanismos de Segurança (RFC 2828)

- Cifragem
  - Dados não legíveis
  - Algoritmo e 0 ou mais chaves
- Assinatura Digital
  - Prova de fonte
  - Prova de integridade
  - Proteção quanto a forjamento
- Controle de Acesso
  - Mecanismos no servidor

Mecanismos de Segurança (RFC 2828)

- Controle de Integridade
- Autenticação
  - De entidades
  - Mútua
    - A autentica-se perante B
    - B autentica-se perante A
- “Padding” de trafego
  - Preenchimento de lacunas com informação inútil
  - Contra análise de trafego

Mecanismos de Segurança (RFC 2828)

- Controle de roteamento
  - Seleciona rotas físicas seguras para determinados dados
  - Mudança de rota quando há suspeita de ameaça
- Notarização
  - Terceira parte confiável

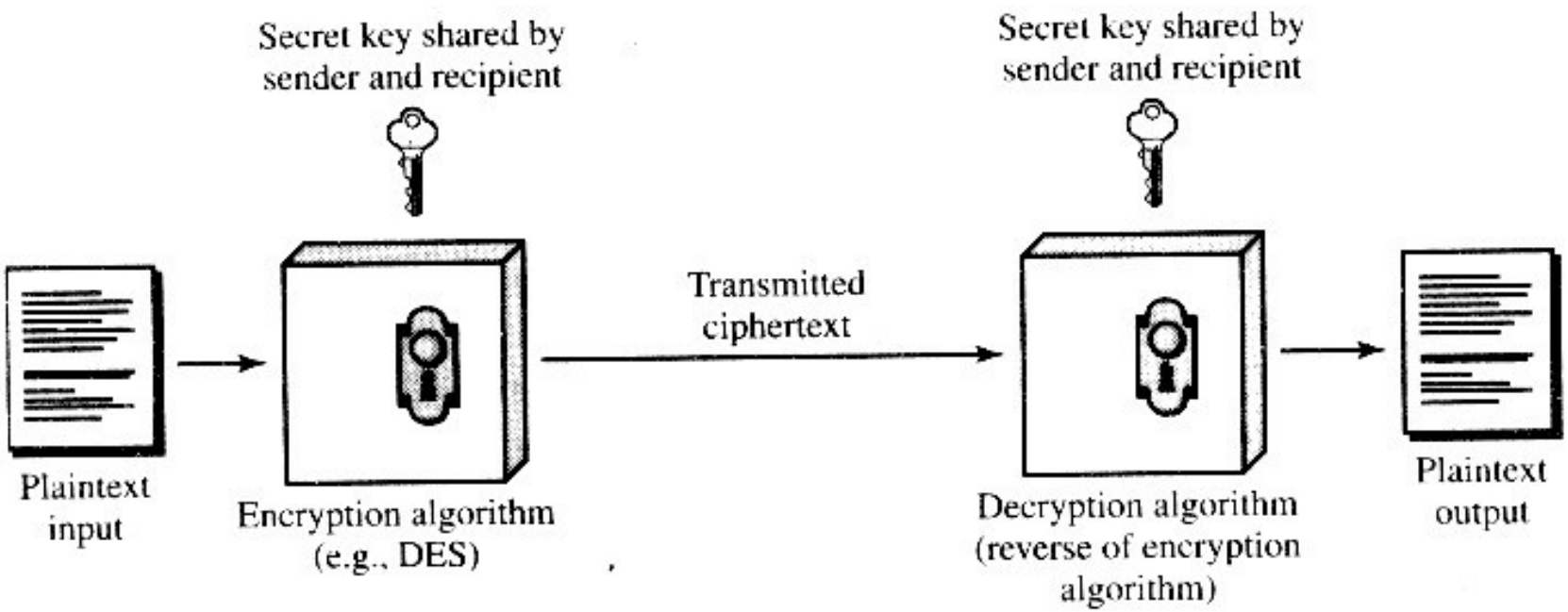
Cifragem – Técnicas Clássicas

- Modelo de Cifragem Simétrica
- Técnicas de Substituição
- Técnicas de Transposição
- Maquinas de Rotores
- Esteganografia

Modelo de Cifragem Simétrica

- Elementos:
  - Texto Claro
  - Algoritmo de Cifração
  - Chave Secreta
  - Texto Cifrado
  - Algoritmo de Decifração
- Algoritmo não é secreto
- Somente conhecendo a chave para conseguir obter informações

Modelo de Cifragem Simétrica



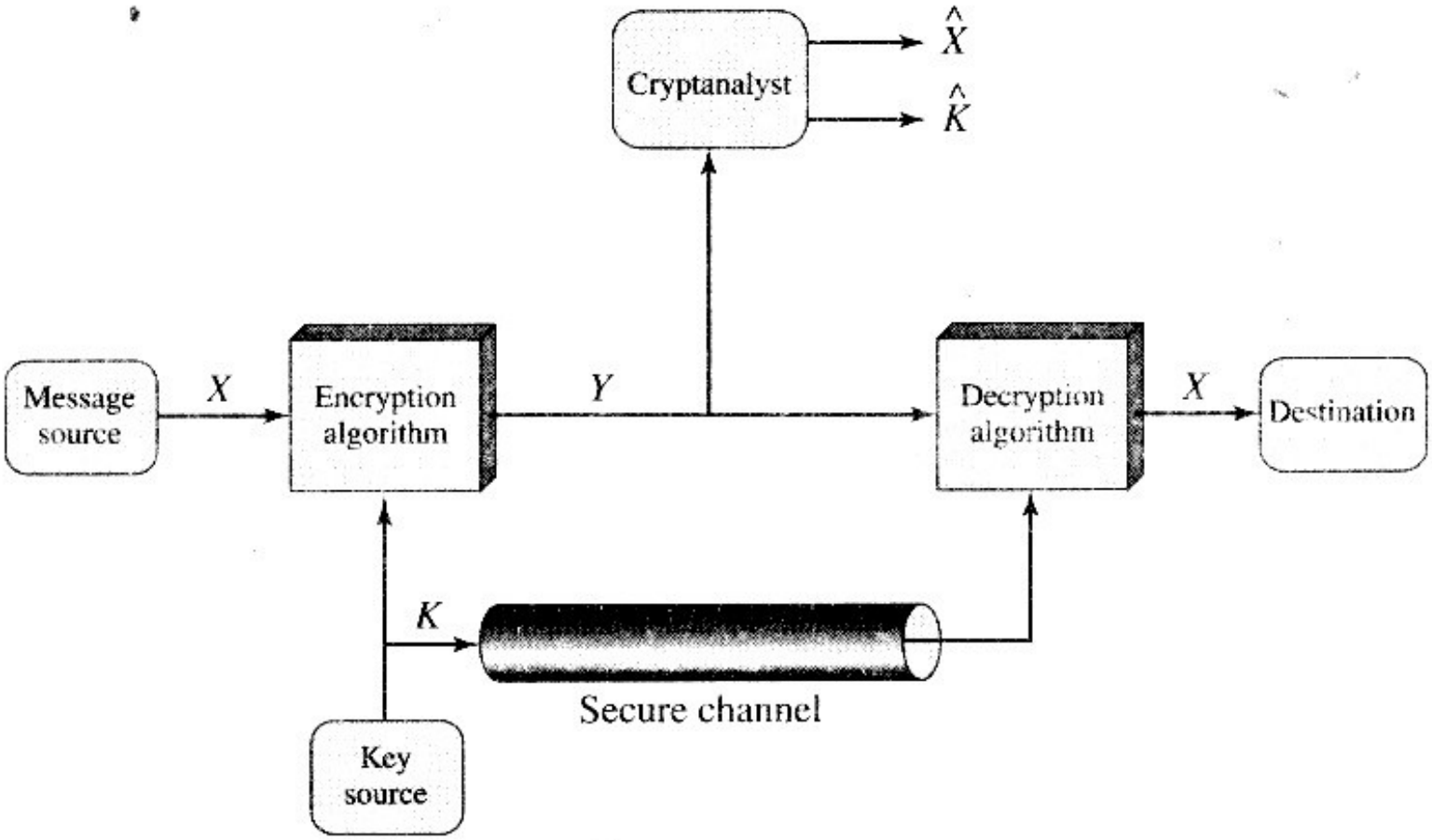
Criptografia x Criptoanálise

- Criptografia
  - Operações no texto claro para texto cifrado
    - Substituição de elementos (mapeamento para outros)
    - Transposição - embaralhamento
  - Numero de Chaves
    - Mesma chave – simétrica
    - Chaves diferentes - assimétrica
  - A forma como o texto claro é processado
    - Bloco
    - Fluxo

Criptografia x Criptoanálise

- Criptoanálise
- Normalmente o objetivo é recuperar a chave
  - Ataque na natureza do algoritmo
    - Características do texto (claro e cifrado)
  - Força Bruta
    - Em média é necessário tentar metade das possíveis chaves antes de suceder

Modelo de Criptosistema simétrico



Criptoanálise

Tipo de Ataque	Acessível ao Criptoanalista
Texto Cifrado Somente	Algoritmo, texto cifrado
Texto Claro Conhecido	Algoritmo Pares texto claro - texto cifrado
Texto Claro Escolhido	Algoritmo Pares texto claro - texto cifrado Texto claro escolhido
Texto Cifrado Escolhido	Algoritmo Pares texto claro-texto cifrado Texto cifrado escolhido
Texto Escolhido	Algoritmo Pares texto claro-texto cifrado Texto claro escolhido Texto cifrado escolhido

Incondicionalmente Seguro
x
Computacionalmente Seguro

- Incondicional
  - Texto cifrado não contém informação suficiente para determinar o texto claro
- Computacional
  - Custo de quebrar excede o valor do conteúdo
  - O tempo requerido é maior que a vida útil do conteúdo

Incondicionalmente Seguro
x
Computacionalmente Seguro

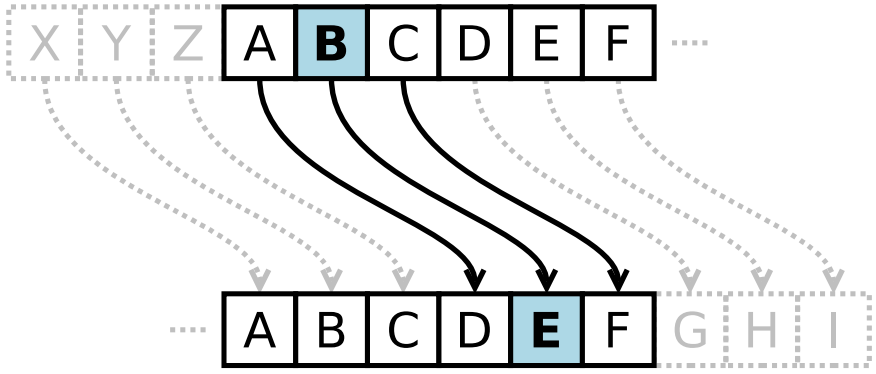
Key size (bits)	Number of alternative keys	Time required at 1 decryption/μs	Time required at 10^6 decryption/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

Técnicas de Substituição

- Cifrador de Cezar
- Cifradores Mono-alfabéticos
- Playfair
- Cifradores Poli-alfabéticos
- Cifrador de Veginère
- Cifrador de Vernam
- One-time pad

Cifrador de Cesar

- Claro: Me encontre depois da aula
- Cifrado: PH HQFRQWUH GHSRLV GD DXOD
- C = (p + 3) mod 26
- Chave = 3
- Criptoanálise:
  - Força Bruta
    - 25 chaves para tentar



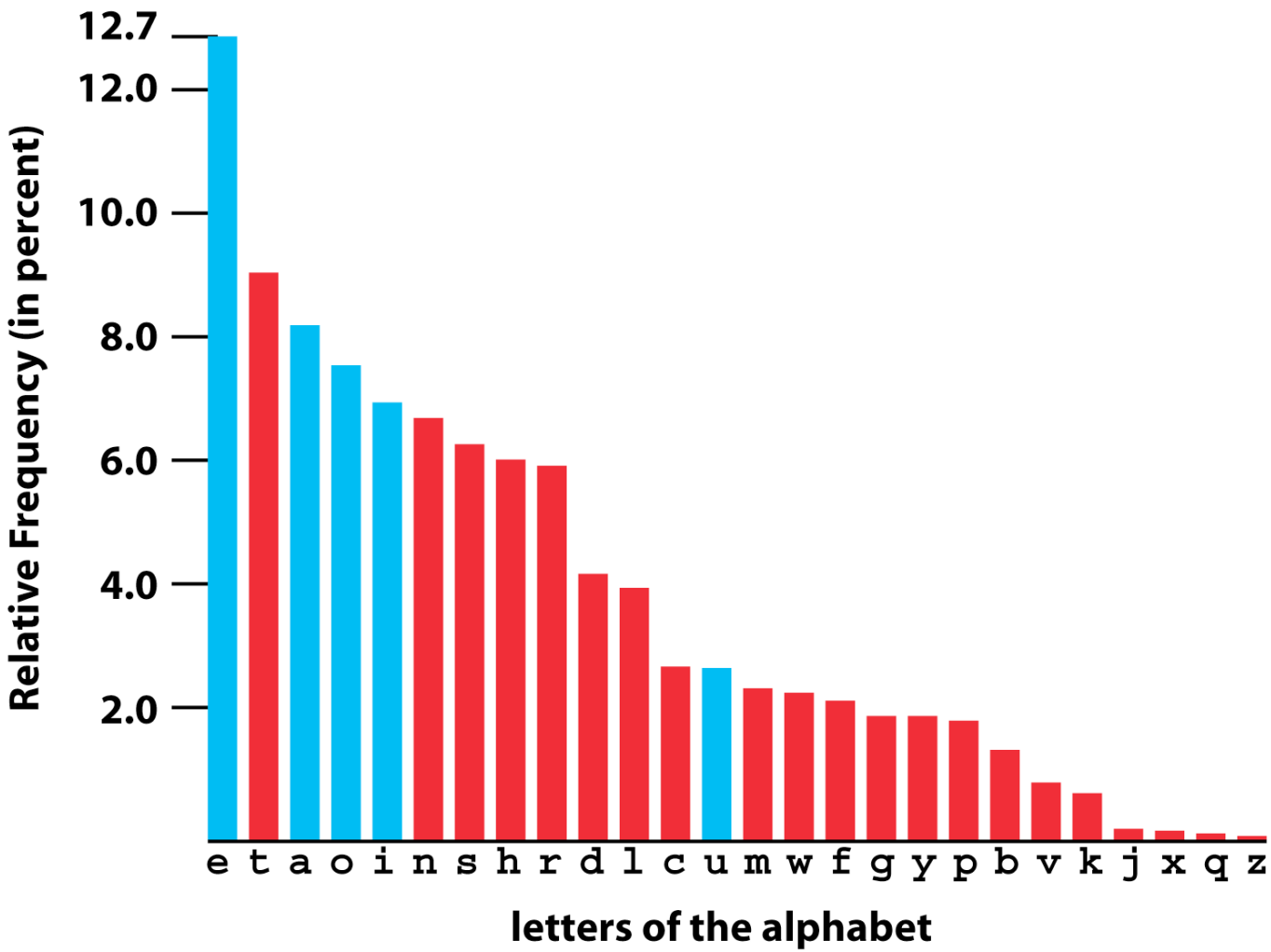
Cifrador de Cesar

- Características que permitem o uso de força bruta:
  - Os algoritmos de cifração e decifração são conhecidos
  - Somente 25 possíveis chaves
  - Linguagem do texto claro conhecida e facilmente reconhecida

Cifradores Mono-alfabéticos

- Mapeia de um alfabeto para outro alfabeto
- Troca de uma letra por outra letra qualquer
- Espaço de Chaves:
  - 26! > 4 x 10 ˆ 26
  - Maior que DES
- Criptoanálise:
  - Análise de freqüência
  - Analise de duplas, triplas

Freqüência Relativa das Letras



Playfair

- Cifra pares de letras
- Mesma linha, coluna do par – CH -> AK
- Pares na mesma linha → Direita
- Pares na mesma coluna → Abaixo
- Esconde digramas (análise de freq. mais difícil)

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

Cifradores Poli-Alfabéticos

- Usam um conjunto de substituições mono-alfabéticas
- Uma chave determina como a transformação é dada
- Ofusca as informações de freqüência
- Nem toda a estrutura é perdida

Cifrador de Veginère

- Chave: seguroseguroseguro
- Claro: aulanosabadoebom
- Cifrado: SYRUECJEHUUWFUG
- Ataque:
  - Determinar o tamanho da chave
  - Distância da repetição no texto cifrado

	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

Cifrador de Veginère

- Chave: deceptive
- Texto: We are dicovered, save yourself

deceptivedeceptivedeceptive

wearediscoveredsaveyourself

ZICVTWQNGRZGVTWAVZHC...

- Chave de tamanho 3 ou 9

Cifrador de Vernam

- Transformação do texto em bits
- Transformação da chave em bits
- Ou-Exclusivo bit a bit
- Ci = Pi ⊕Ki
- Ataque:
  - Análise de frequência não funciona
  - Alfabeto pequeno para fazer inferências

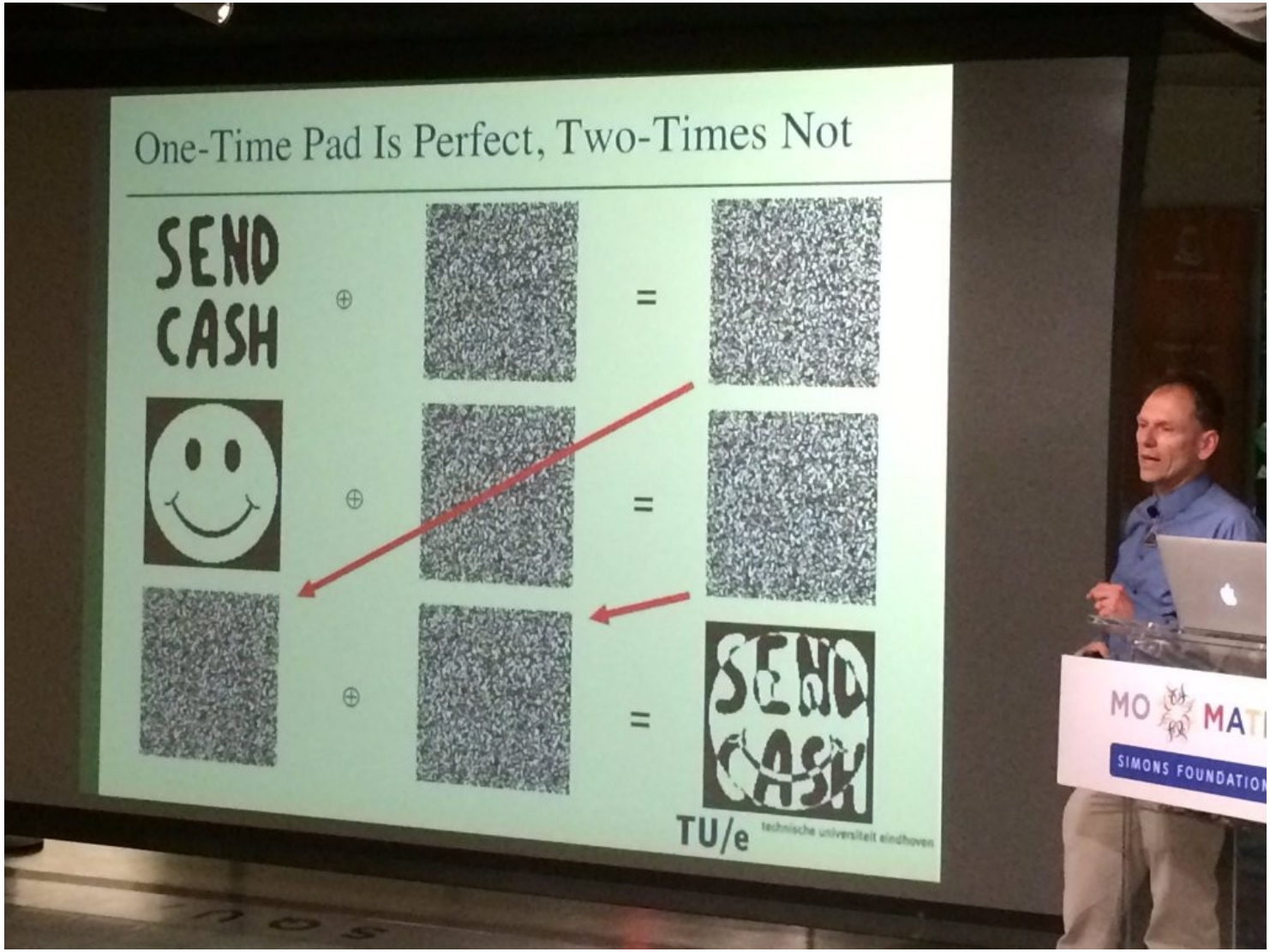
One-Time Pad

- Chave de igual tamanho ao texto claro
- Chave verdadeiramente aleatória
- Incondicionalmente seguro
- Cifrador de Veginère:

```
ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext:  mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        mfugpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt
plaintext:  miss scarlet with the knife in the library
```

One-Time Pad (@MoMath1)



Técnicas de Transposição

- Permutação no texto claro
- C i t g a i e a i
- R p o r f a f c l
- Matriz escrita em linha e recuperada em colunas
  - Chave pode ser a ordem das colunas
- Varias permutações confundem a Criptoanálise

Técnicas de Transposição

4 3 1 5 2

E S T A E

U M A A U

L A D E S

E G U R A

N C A X X

Cítala grega

TADUAEUSAXEMAGCEULENAAERX

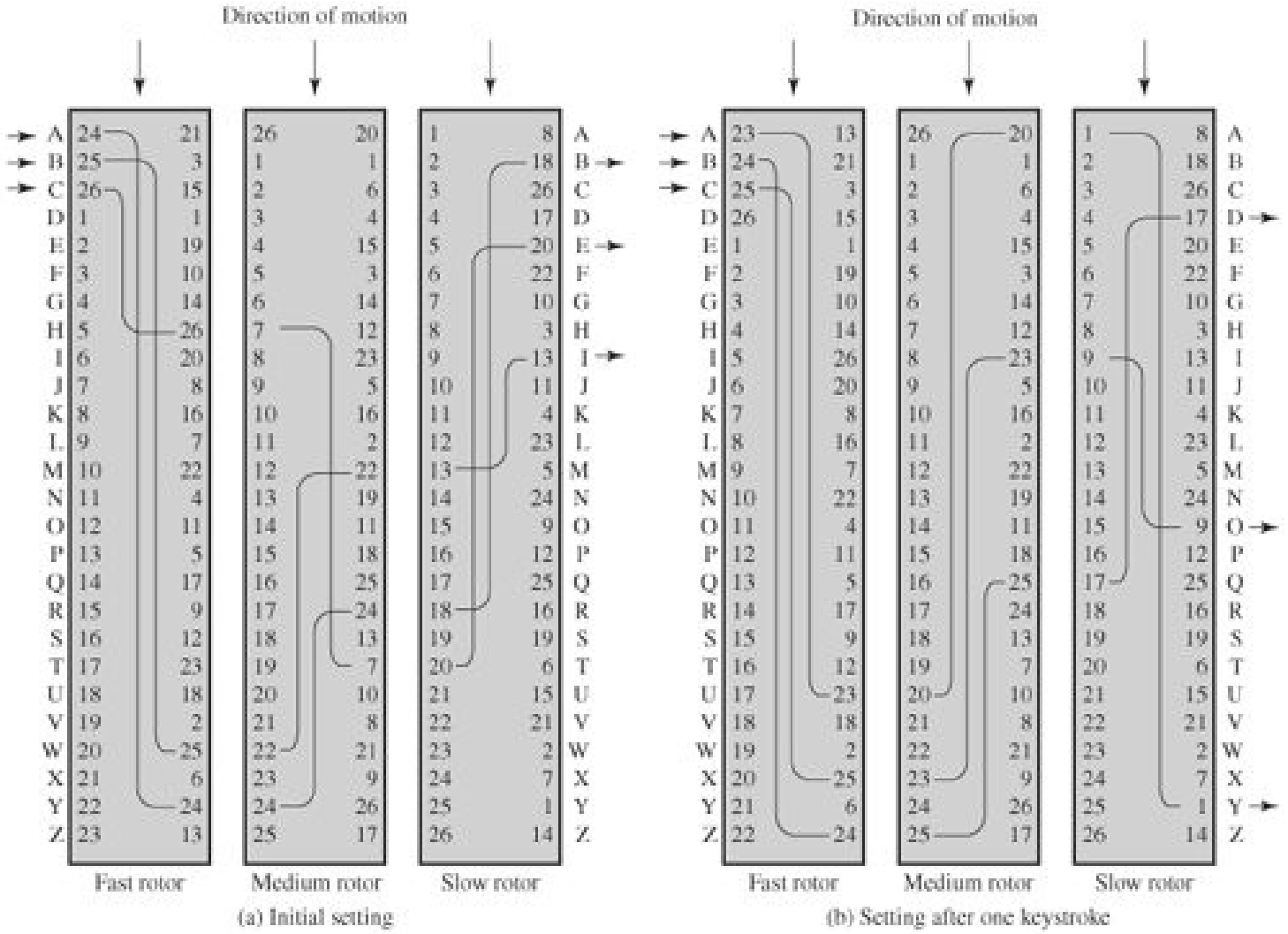
Técnicas de Transposição

- Mesma frequência do texto claro
  - Fácil de reconhecer
- Fácil de reverter se for somente uma permutação
- Transposição do texto cifrado
  - Realizar a transposição de novo com a mesma chave

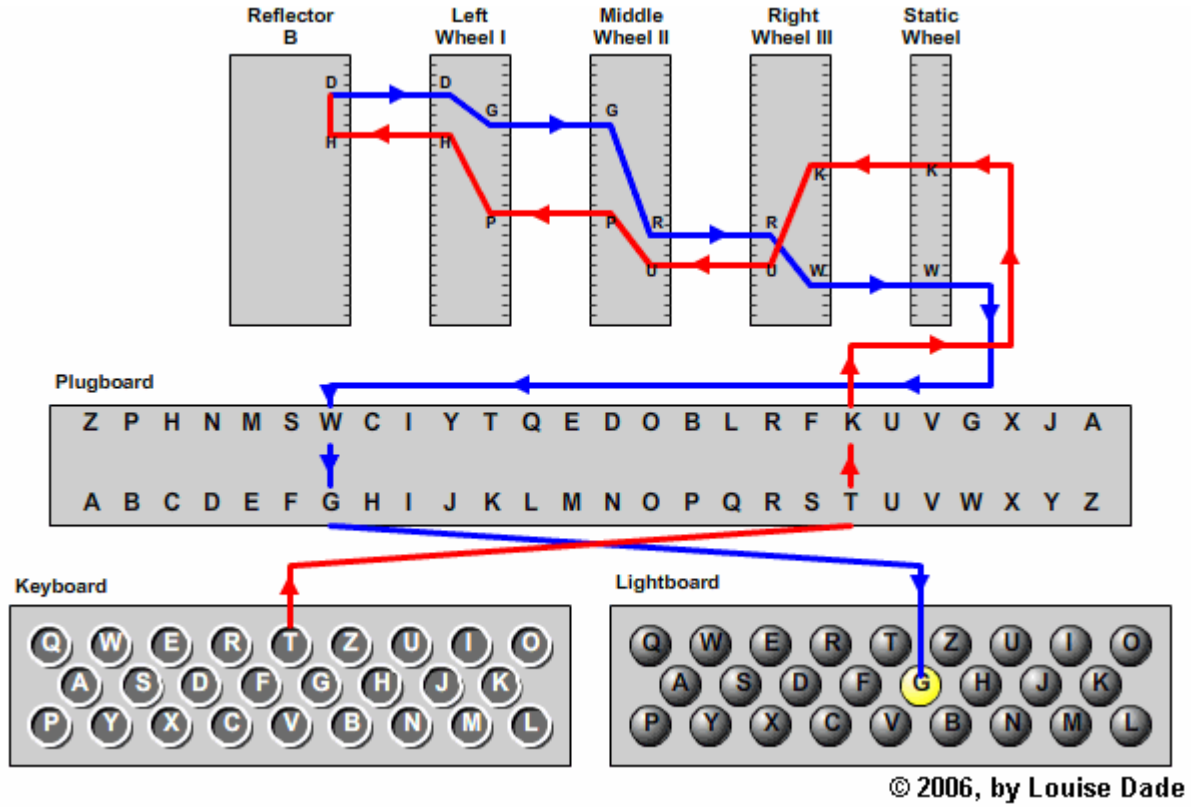
Maquinas de Rotores

- Sistema eletro-mecânico
- Conjunto de cilindros independentes
- Cada cilindro um cifrador mono-alfabético
- Chave:
  - Posição inicial dos rotores, posição do alfabeto, retroalimentação

Maquinas de Rotores



Maquinas de Rotores



Maquinas de Rotores

Maquinas de Rotores

- Cada volta completa do primeiro rotor faz o rotor do meio gira um pino
- Cada volta completa do rotor do meio faz o último rotor girar um pino

26 x 26 x 26 = 17.576 substituições

Esteganografia

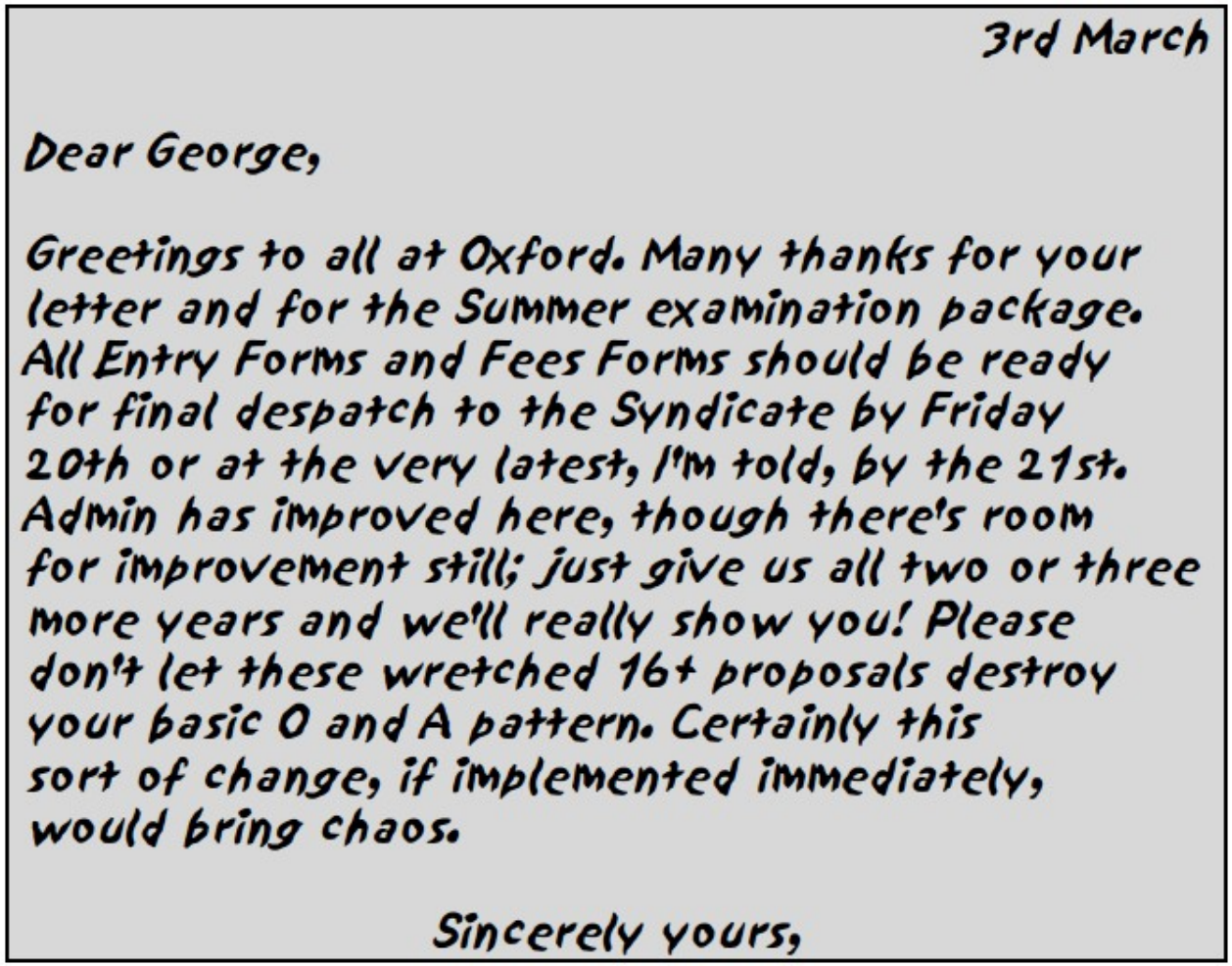
- Mensagem escondida em mídia portadora
- Objetivo: Repúdio do Envio
- Técnicas clássicas:
  - Marcação de caracteres
  - Tinta invisível
- Técnicas Modernas
  - Imagens
  - Audio

Esteganografia

- A imagem escondida foi obtida através dos dois últimos bits de cada componente de cor

Esteganografia

- Qual é a mensagem escondida?



3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours,