INSTITUTO FEDERAL DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA
PARAÍBA

# Introdução à Criptografia

Dênio Mariz, Dr.
denio@ifpb.edu.br

Março, 2019

# Segurança da Informação: Objetivos e Requisitos

- Integridade
  - Manutenção do estado da informação, comprovando que não foi modificada enquanto armazenada ou em trânsito
- Confidencialidade
  - Garantia de que apenas pessoas autorizadas tenham acesso a informação
- Autenticação
  - Confirmação da identidade de uma pessoa ou dispositivo
  - Autenticação de mensagem: quando a parte receptora pode verificar a origem da mensagem
- Não repúdio (irrefutabilidade)
  - O autor de uma informação não pode contestar com êxito sua autoria ou validade.
- Disponibilidade
  - Garantia que a informação estará disponível quando necessária
  - Muito relacionado com infraestrutura

Criptografia

# Criptografia

- Criptografia, Criptologia
  - A prática e estudo de técnicas para comunicação segura (confidencial) na presença terceiros
- Etimologia
  - Do grego kryptós (escondido, secreto) e graphein (escrita)

# Sistemas Criptográficos

- Criptografia Simétrica: UMA chave **compartilhada**
  - Existe simetria: a chave é a mesma para cifrar e decifrar
  - A chave é compartilhada com ambos os lados da comunicação
- Criptografia Assimétrica: DUAS chaves
  - Chave pública = compartilhada
  - Chave privada = nunca compartilhada
  - Se uma cifra, a outra decifra (qualquer ordem)

- Em ambos os tipos
  - A chave é o segredo, não o algoritmo! (Kerckhoffs's principle)

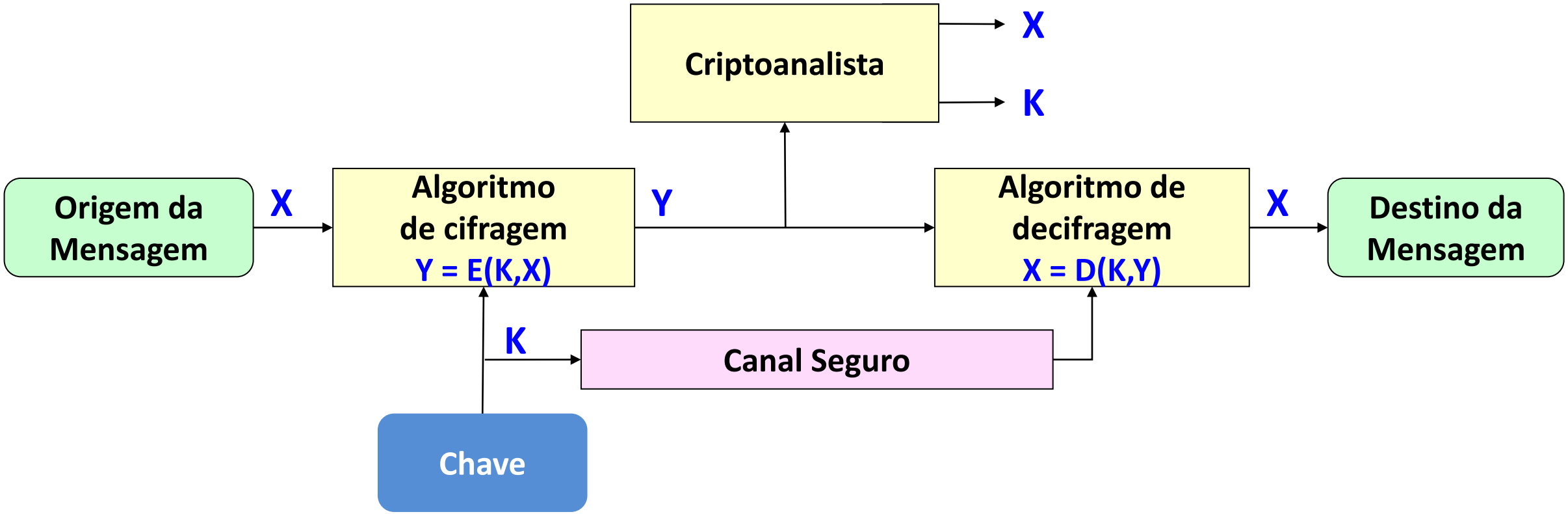
# Terminologia

- Quem envia? Alice
- Quem recebe? Bob
- Um terceiro no meio: Maria
- Um terceiro confiável: Ted (trusted)
- Funções
  - Cifrar e Decifrar OU
  - Encriptar e Decriptar OU
  - Criptografar e Decriptografar
- Mensagem Original: TEXTO PLANO (plain text/clear text)
- Mensagem resultante: TEXTO CIFRADO (cipher text)

# Terminologia (sistema simétrico)

- Notação usada:
  - X – Texto Plano
  - Y – Texto Cifrado
  - E – Função para cifragem (encryption)
  - D – Função para decifragem (decryption)
  - K – Chave
- Assim: Y = E(K,X) e X = D(K,Y)

# Sistema Criptográfico Simétrico




Obs: O texto cifrado Y não contém informações sobre a chave K

# Técnica 1: Substituição Monoalfabética 1/2

- Uma letra é substituída por outra
- Cifrador de Julius Caesar
  - Chave é um inteiro
  - Cada letra é somada com a chave

- Exemplo: chave=3

```
PlainText:  IMPETUM GERMANIAE MERIDIONALIS
CipherText: LPSHWXP JHUPDQLDH PHULGLRQDOLV
```

# Técnica 1: Substituição Monoalfabética

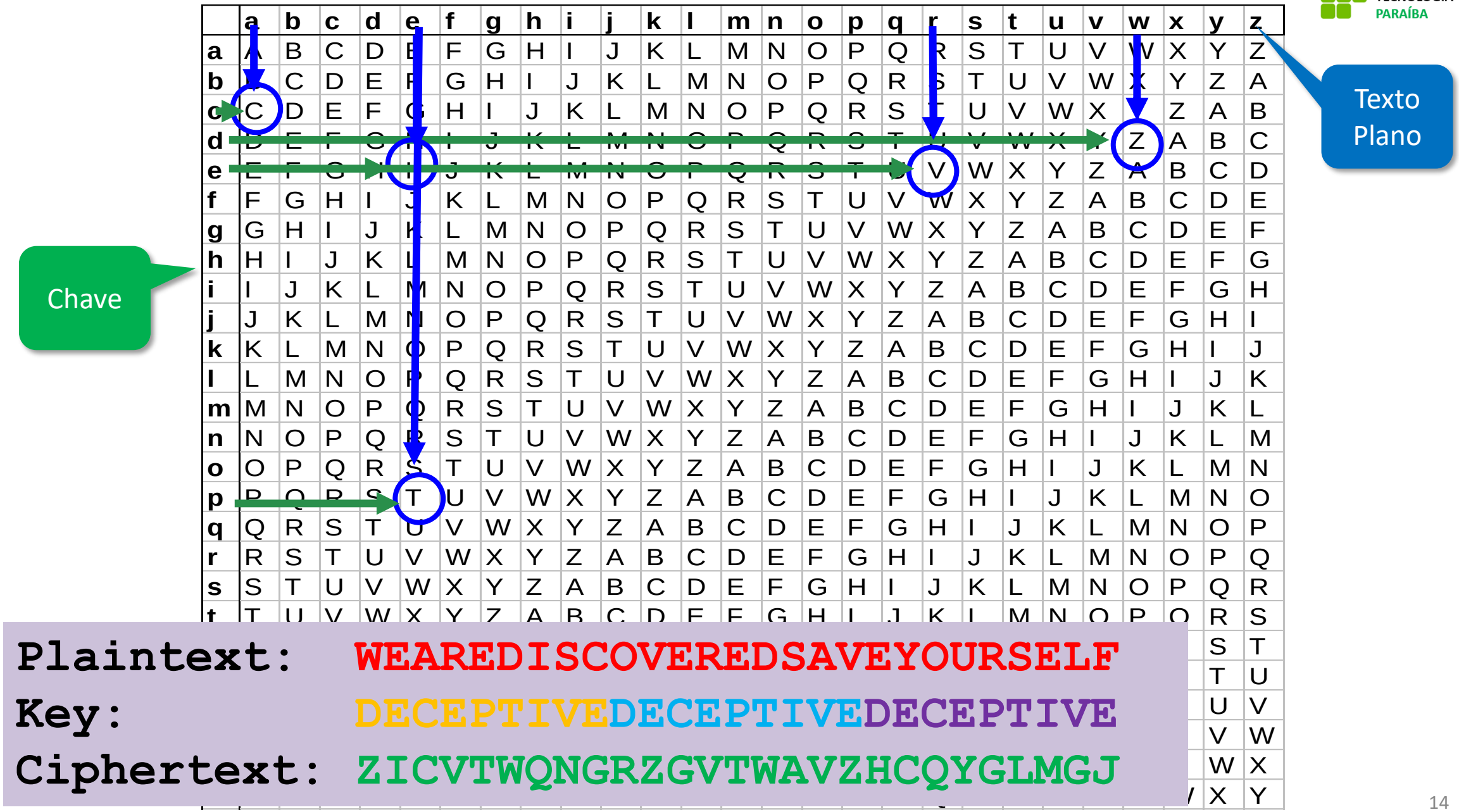
- Forma geral do Algoritmo de Julius Caesar
  - Considerando a=1, b=2, ..., z=26
  - Para cada letra X, substitua pela letra cifrada Y
  - Cifrar: $Y=E(X)=(X-1+K) \bmod 26 + 1$
  - Decifrar: $X=D(Y)=(Y-K-1) \bmod 26 + 1$

- Questão: com quantas tentativas se quebra o algoritmo de Caesar ?

# Técnica 1: Substituição Monoalfabética 2/2

- Cifrador de Vigenère
  - A chave é um texto
  - Chave é combinada com texto plano
- Exemplo:
  - Chave = “DECEPTIVE”
  - Texto Plano: “WE ARE DISCOVERED SAVE YOURSELF”
  - Algoritmo: (vide tabela adiante)

```
Plaintext:   WEAREDISCOVEREDSAVEYOURSELF
Key:         DECEPTIVEDECEPTIVEDECEPTIVE
Ciphertext:  ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```




| | 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 |

**Plaintext:** WEAREDISCOVEREDSAVEYOURSELF

**Key:** DECEPTIVEDECEPTIVEDECEPTIVE

**Ciphertext:** ZICVTWQNGRZGVTWAVZHCQYGLMGJ

# Quebrando a Substituição Monoalfabética

- Considere o texto em Inglês cifrado abaixo

```
UZ QSO VUOHXMOPV UGATERGPO EVSG ZWSZOPF PESXUDBM ETS
XAIZVU HZHDMZSH ZOWS FPAP PDTS TRRE VPQUZWYMX
UZUHSXEPYEPOPDZ SZ UFP OMBZ WPFU PZ HMDJUD
```

- e a frequência de ocorrência das letras

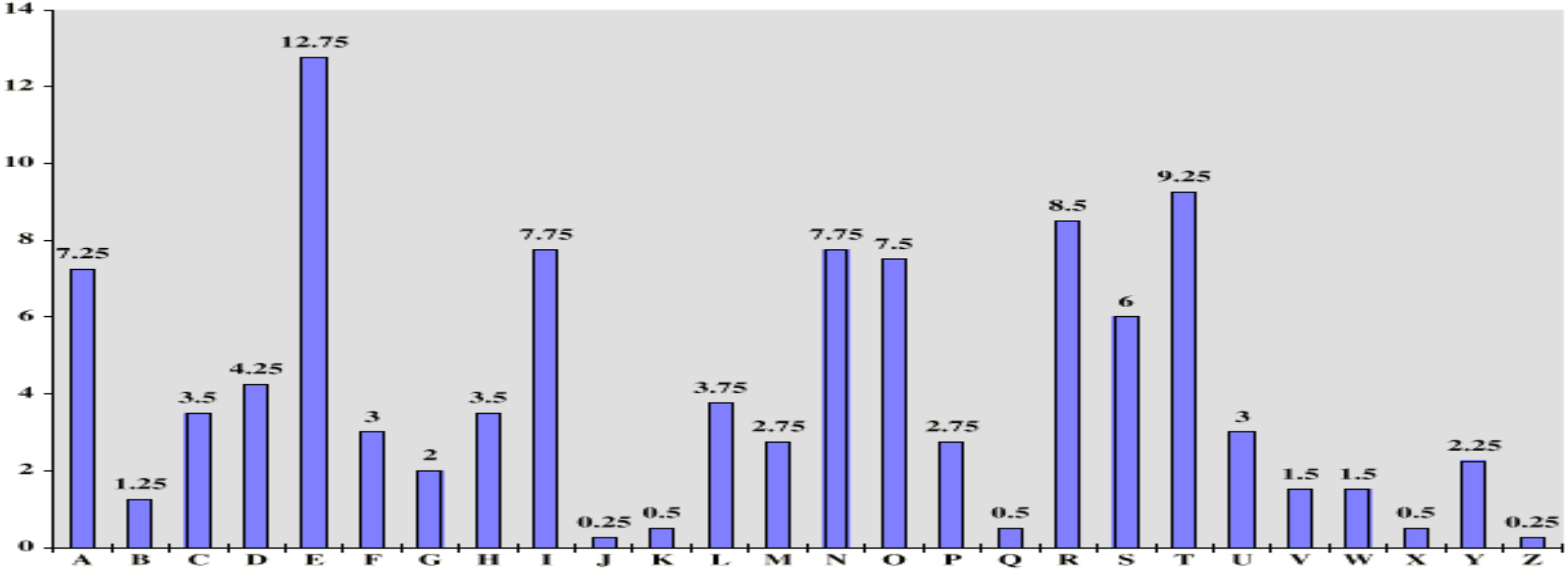
| | | | | |
|---|---|---|---|---|
| P 13, 33 | H 5, 83 | F 3, 33 | B 1, 67 | C 0, 00 |
| Z 11, 67 | D 5, 00 | W 3, 33 | G 1, 67 | K 0, 00 |
| S 8, 33 | E 5, 00 | Q 2, 50 | Y 1, 67 | L 0, 00 |
| U 8, 33 | V 4, 17 | T 2, 50 | I 0, 83 | N 0, 00 |
| O 7, 50 | X 4, 17 | A 1, 67 | J 0, 83 | R 0, 00 |
| M 6,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

# Quebrando a Substituição Monoalfabética

- Substituição monoalfabética pode ser criptoanalisada por métodos estatísticos
- Estatisticamente pode-se inferir um parâmetro ē populacional a partir de ê amostral...
- Traduzindo...
  - Sabendo-se a frequência relativa das letras de uma língua, pode-se deduzir que substituições foram feitas, sem necessariamente saber a tabela de permutação

# Quebrando a Substituição Monoalfabética

- Considere também a frequência das letras de textos em Inglês (amostral ~ populacional)



# Quebrando a Substituição Monoalfabética

➔O texto abaixo

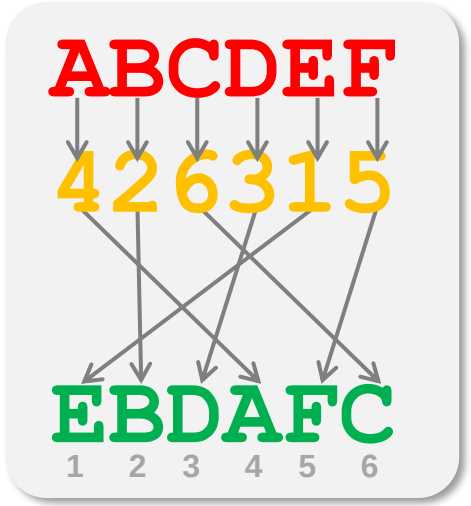
```
UZ QSO VUOHXMOPV UGATERGPO EVSG ZWSZOPF PESXUDBM ETS
XAIZVU HZHDMZSH ZOWS FPAP PDTS TRRE VPQUZWYMX
UZUHSXEPYEPOPDZ SZ UFP OMBZ WPFU PZ HMDJUD
```

➔foi decifrado como

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

# Técnica 2: Transposição

- Cada caractere permanece inalterado, mas troca de posição
- Exemplo:
  - Chave: 426315 (bloco de 6 caracteres)
  - Posição 1 vai para 4, posição 2 vai para 2, posição 3 vai para 6 ...




```
Plaintext:   WE ARE DISCOVERED SAVE YOURSELF*****
Key:         426315426315426315426315426315426315
Ciphertext:  REAWE CDS OIDEEV R AESYVEUSOLR***F**
```

# Técnicas de Criptografia Clássicas

- Máquina dos Três Rotores
- Composta por:
  - Conjunto de três cilindros independentes
  - Cada cilindro tem 26 entradas e 26 saídas
  - Ao associar uma entrada a uma letra temos um cifrador monoalfabético
  - Múltiplos cilindros implica em polialfabético

# Enigma Cipher Machine

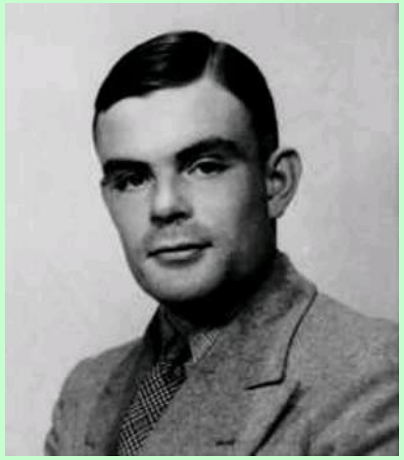
- Máquina de criptografia com "rotores" foi inventada pelo engenheiro alemão Arthur Scherbius em 1918 para cifrar mensagens na área de finanças.
- Adotada e melhorada pelo exército alemão. Usada durante a WWII com o nome de "Enigma".
- Usa substituição + transposição (difusão).
- Criptografia simétrica.
- Quebrada pelos aliados em 1940.

# Enigma Cipher Machine

# A “quebra” da Enigma Cipher Machine

- Durante a guerra (1938-1945) aliados decifraram 50 mil mensagens
- 2 mil mensagens eram interceptadas por dia (total de 5 milhões no período)
- Eficiência de 1% na quebra das mensagens cifradas

**Marian Rejewski**, matemático polonês que “criptoanalisou" a Enigma em 1932



**Alan Turing**, matemático inglês que automatizou a quebra da Enigma

Center for Cryptologic History - http://www.nsa.gov/cch

FULL CAST AND CREW | TRIVIA | USER REVIEWS | IMDbPro | MORE | SHARE

# O Jogo da Imitação (2014)

8,0/10 669.678 | Rate This

The Imitation Game *(original title)*

12 | 1h 54min | Biography, Drama, Thriller | 5 February 2015 (Brazil)


2:26 | Trailer 6 VIDEOS | 200 IMAGES

During World War II, the English mathematical genius Alan Turing tries to crack the German Enigma code with help from fellow mathematicians.

EN

**Director:** Morten Tyldum
**Writers:** Graham Moore, Andrew Hodges (book)
**Stars:** Benedict Cumberbatch, Keira Knightley, Matthew Goode | See full cast & crew »

# Referências


- en.wikipedia.org/wiki/TypeX
- en.wikipedia.org/wiki/SIGABA
- en.wikipedia.org/wiki/History_of_cryptography
- Cryptography FAQ, www.x5.net/faqs/crypto/
- Center for Cryptologic History (National Security Agency, USA), http://www.nsa.gov/cch