Introdução à Criptografia

Auditoria e Segurança de SI

Prof. Roberto Cabral

rbcabral@ufc.br

Universidade Federal do Ceará

1º semestre/2023

Criptografia

- O que vem a sua cabeça ao ouvir a palavra **Criptografia?**

Criptografia

- O que vem a sua cabeça ao ouvir a palavra **Criptografia?**
  - Encriptação de email?

Criptografia

- O que vem a sua cabeça ao ouvir a palavra **Criptografia?**
  - Encriptação de email?
  - Segurança de sites webs?

Criptografia

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- O que vem a sua cabeça ao ouvir a palavra **Criptografia?**
  - Encriptação de email?
  - Segurança de sites webs?
  - Aplicações bancarias?

Introdução

- Dado esses exemplos, a criptografia parece intimamente ligada à comunicação eletrônica moderna.

Introdução

- Dado esses exemplos, a criptografia parece intimamente ligada à comunicação eletrônica moderna.
- Mas a criptografia é bastante antiga, com relatos desde 2000 A.C.

Introdução

- Dado esses exemplos, a criptografia parece intimamente ligada à comunicação eletrônica moderna.
- Mas a criptografia é bastante antiga, com relatos desde 2000 A.C.
- Existe indícios de uso da criptografia na maiorias das culturas que desenvolveram a escrita.

Introdução

- Dado esses exemplos, a criptografia parece intimamente ligada à comunicação eletrônica moderna.
- Mas a criptografia é bastante antiga, com relatos desde 2000 A.C.
- Existe indícios de uso da criptografia na maiorias das culturas que desenvolveram a escrita.
  - Espartanos com uma Scytale.

Introdução

- Dado esses exemplos, a criptografia parece intimamente ligada à comunicação eletrônica moderna.
- Mas a criptografia é bastante antiga, com relatos desde 2000 A.C.
- Existe indícios de uso da criptografia na maiorias das culturas que desenvolveram a escrita.
  - Espartanos com uma Scytale.
  - Cifra de César.

Definições

Definição clássica

Etimologicamente, criptografia é a **arte da escrita secreta**.

Definições

Definição clássica

Etimologicamente, criptografia é a **arte da escrita secreta**.

Definição moderna

Criptografia é a arte/ciência/engenharia que estuda técnicas para fornecimento de serviços de segurança, como sigilo, autenticação de origem, anonimato, integridade e irretratabilidade, primordialmente em sistemas computacionais.

Definições

Definição clássica

Etimologicamente, criptografia é a **arte da escrita secreta**.

Definição moderna

Criptografia é a arte/ciência/engenharia que estuda técnicas para fornecimento de serviços de segurança, como sigilo, autenticação de origem, anonimato, integridade e irretratabilidade, primordialmente em sistemas computacionais.

Criptoanálise

Refere-se ao conjunto de técnicas para **analisar** métodos criptográficos.

Definições

Definição clássica

Etimologicamente, criptografia é a **arte da escrita secreta**.

Definição moderna

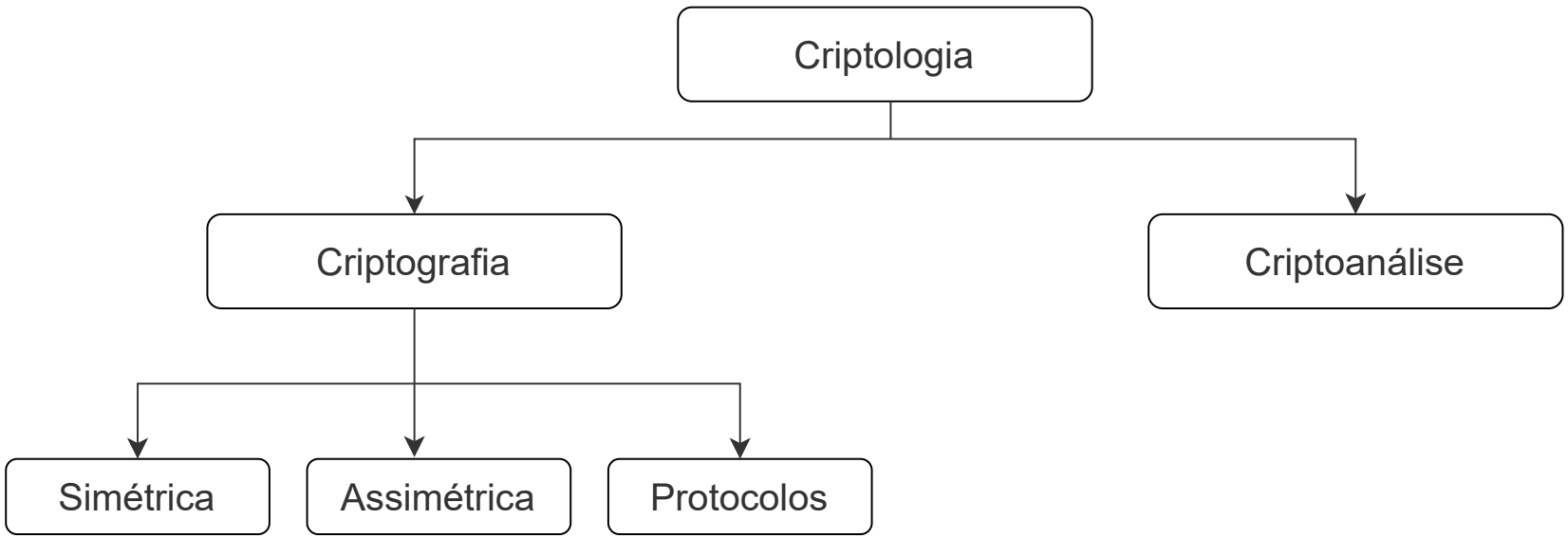
Criptografia é a arte/ciência/engenharia que estuda técnicas para fornecimento de serviços de segurança, como sigilo, autenticação de origem, anonimato, integridade e irretratabilidade, primordialmente em sistemas computacionais.

Criptoanálise

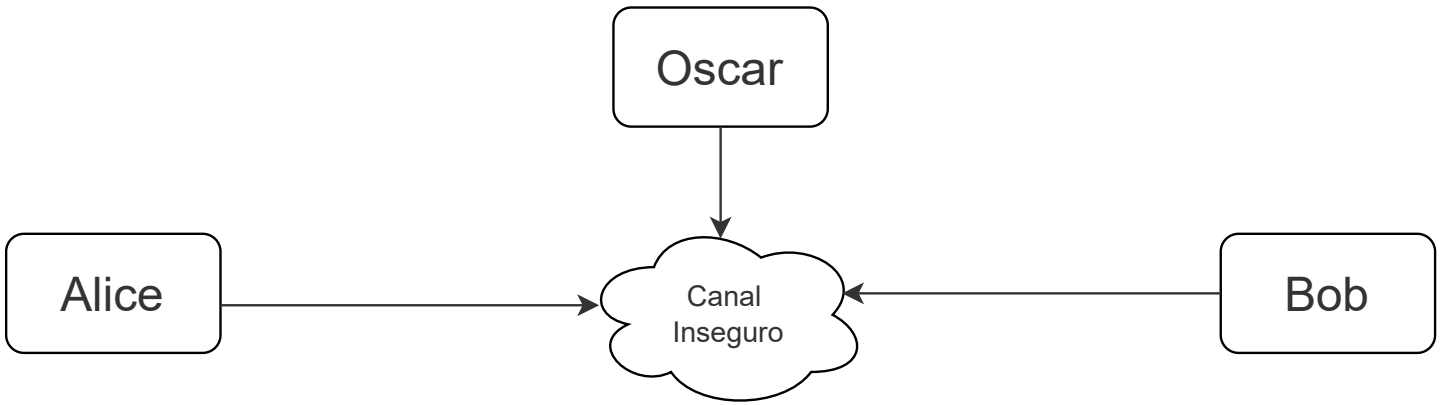
Refere-se ao conjunto de técnicas para **analisar** métodos criptográficos.

$$\text{Criptologia} = \text{Criptografia} + \text{Criptoanálise}$$

Campos da Criptografia



Comunicação por meio de um canal inseguro



Criptosistema simétrico

- Os algoritmos de encriptação simétricos são usualmente conhecidos por `cifras` e compartilham uma chave de encriptação K.
- Uma cifra é composta por algoritmos de encriptação e decriptação.
- Um algoritmo de `encriptação` (E) transforma um **texto claro** (P) em um **texto encriptado** (C).
- Um algoritmo de `dencriptação` (D) transforma um texto encriptado em um texto claro.
- Sistema simétrico:
  - Encriptação: $C = E(K, P)$
  - Decriptação: $P = D(K, C)$

Comentários

- Nesse cenário, tanto o algoritmo de encriptação como o de decriptação devem ser de conhecimento público!

Comentários

- Nesse cenário, tanto o algoritmo de encriptação como o de decriptação devem ser de conhecimento público!
- A única forma de saber se um algoritmo é seguro é o tornando público para ser analisado por outros criptógrafos.

Comentários

- Nesse cenário, tanto o algoritmo de encriptação como o de decriptação devem ser de conhecimento público!
- A única forma de saber se um algoritmo é seguro é o tornando público para ser analisado por outros criptógrafos.
- **A única coisa que deve ser mantida em segredo nesse tipo de criptosistema é a chave.**

Cifra de substituição monoalfabética

Definição

Uma substituição monoalfabética $e_\pi : \mathcal{P} \to \mathcal{C}$ é uma regra para substituir cada caractere x_i da mensagem x por $\pi(x_i)$, onde π define uma permutação no alfabeto de definição.

Cifra de substituição monoalfabética

Definição

Uma substituição monoalfabética $e_\pi : \mathcal{P} \to \mathcal{C}$ é uma regra para substituir cada caractere x_i da mensagem x por $\pi(x_i)$, onde π define uma permutação no alfabeto de definição.

- Exemplo:

Cifra de substituição monoalfabética

Definição

Uma substituição monoalfabética $e_\pi : \mathcal{P} \to \mathcal{C}$ é uma regra para substituir cada caractere x_i da mensagem x por $\pi(x_i)$, onde π define uma permutação no alfabeto de definição.

- Exemplo:
  - $A \to k$

Cifra de substituição monoalfabética

Definição

Uma substituição monoalfabética $e_\pi : \mathcal{P} \to \mathcal{C}$ é uma regra para substituir cada caractere x_i da mensagem x por $\pi(x_i)$, onde π define uma permutação no alfabeto de definição.

- Exemplo:
  - $A \to k$
  - $B \to d$

Cifra de substituição monoalfabética

Definição

Uma substituição monoalfabética $e_\pi : \mathcal{P} \to \mathcal{C}$ é uma regra para substituir cada caractere x_i da mensagem x por $\pi(x_i)$, onde π define uma permutação no alfabeto de definição.

- Exemplo:
  - $A \to k$
  - $B \to d$
  - $C \to w$

Cifra de substituição monoalfabética

Definição

Uma substituição monoalfabética $e_\pi : \mathcal{P} \to \mathcal{C}$ é uma regra para substituir cada caractere x_i da mensagem x por $\pi(x_i)$, onde π define uma permutação no alfabeto de definição.

- Exemplo:
  - $A \to k$
  - $B \to d$
  - $C \to w$
  - ...

Exemplo

- Mensagem Encriptada:

Exemplo

- Mensagem Encriptada:
  - TW LGW ZKALOSTOKG, YOSIG RG FGKRTLMT, LGW EAZKA RA HTLMT, LGW RG ETAKA.

Exemplo

- Mensagem Encriptada:
  - TW LGW ZKALOSTOKG, YOSIG RG FGKRTLMT, LGW EAZKA RA HTLMT, LGW RG ETAKA.

- Mensagem em claro:

Exemplo

- Mensagem Encriptada:
  - TW LGW ZKALOSTOKG, YOSIG RG FGKRTLMT, LGW EAZKA RA HTLMT, LGW RG ETAKA.

- Mensagem em claro:
  - EU SOU BRASILEIRO, FILHO DO NORDESTE, SOU CABRA DA PESTE, SOU DO CEARA.

Exemplo

- Mensagem Encriptada:
  - TW LGW ZKALOSTOKG, YOSIG RG FGKRTLMT, LGW EAZKA RA HTLMT, LGW RG ETAKA.

- Mensagem em claro:
  - EU SOU BRASILEIRO, FILHO DO NORDESTE, SOU CABRA DA PESTE, SOU DO CEARA.

- Chave: AZERTYUIOPQSDFGHJKLMWXCVBN.

Força bruta

- Um atacante tem um texto encriptado e um pedaço de um texto claro.

Força bruta

- Um atacante tem um texto encriptado e um pedaço de um texto claro.
- O atacante decripta um pedaço do texto encriptado com todas as chaves possíveis.

Força bruta

- Um atacante tem um texto encriptado e um pedaço de um texto claro.
- O atacante decripta um pedaço do texto encriptado com todas as chaves possíveis.
- Se o resultado da decriptação for igual ao texto claro, ele potencialmente encontrou a chave correta.

Força bruta

- Um atacante tem um texto encriptado e um pedaço de um texto claro.
- O atacante decripta um pedaço do texto encriptado com todas as chaves possíveis.
- Se o resultado da decriptação for igual ao texto claro, ele potencialmente encontrou a chave correta.

Definição

Seja (x, y) um par de texto claro e texto encriptado, e seja $\mathcal{K}$ o espaço de chaves. Um ataque de força bruta verifica para todo $k_i \in \mathcal{K}$ se:

$$d_{k_i}(y_i) = x.$$

Se a igualdade aparecer, uma possível chave foi encontrada; caso contrário, continue com uma outra chave.

Força bruta

- Na prática, ataques de força bruta podem ser mais complicados por causa de chaves incorretas que podem dar falso positivos.

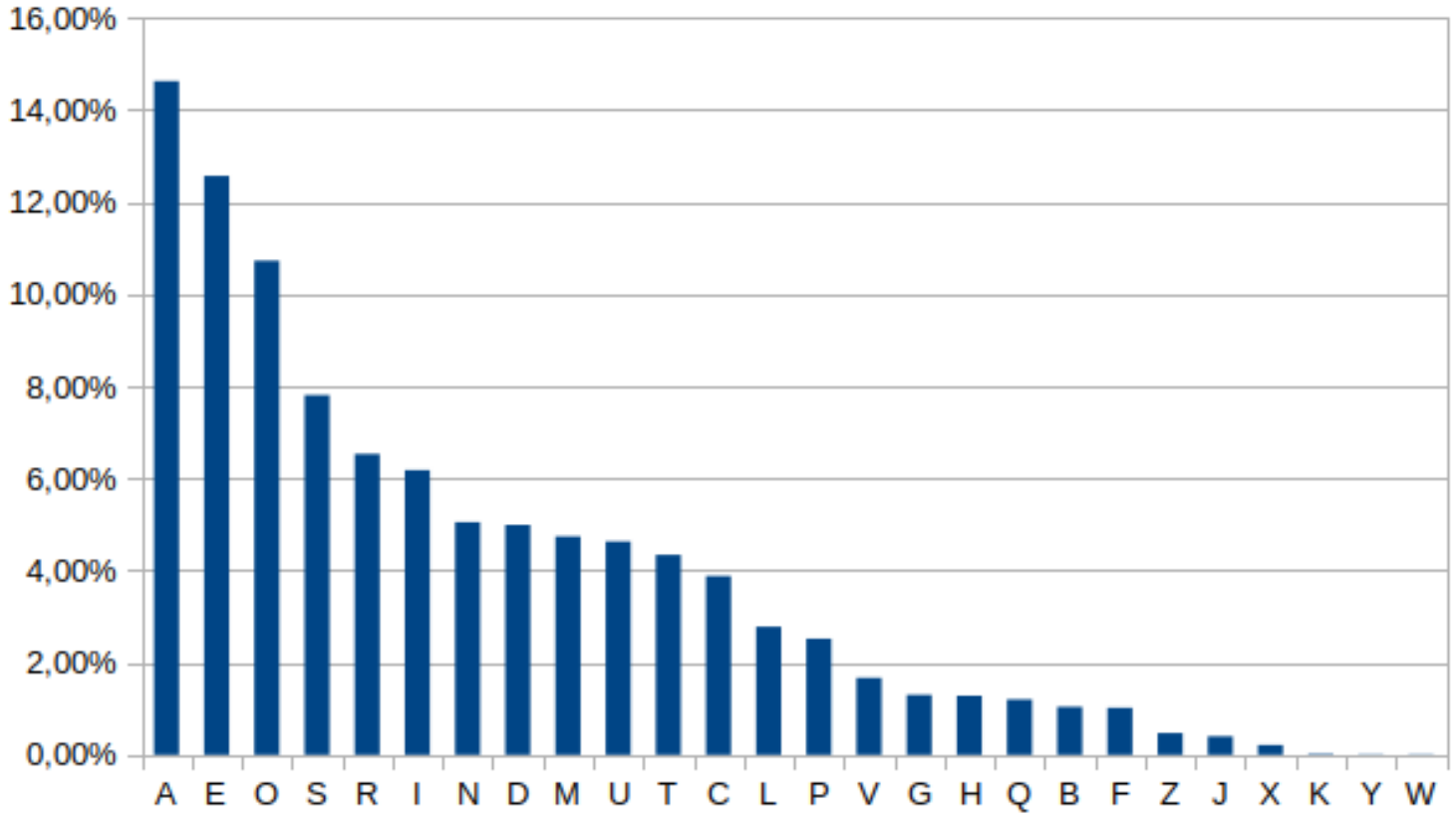
Força bruta

- Na prática, ataques de força bruta podem ser mais complicados por causa de chaves incorretas que podem dar falso positivos.
- Tecnicamente, sempre é possível usar um ataque de força bruta a um criptosistemas simétrico. Mas pode não ser possível na prática.

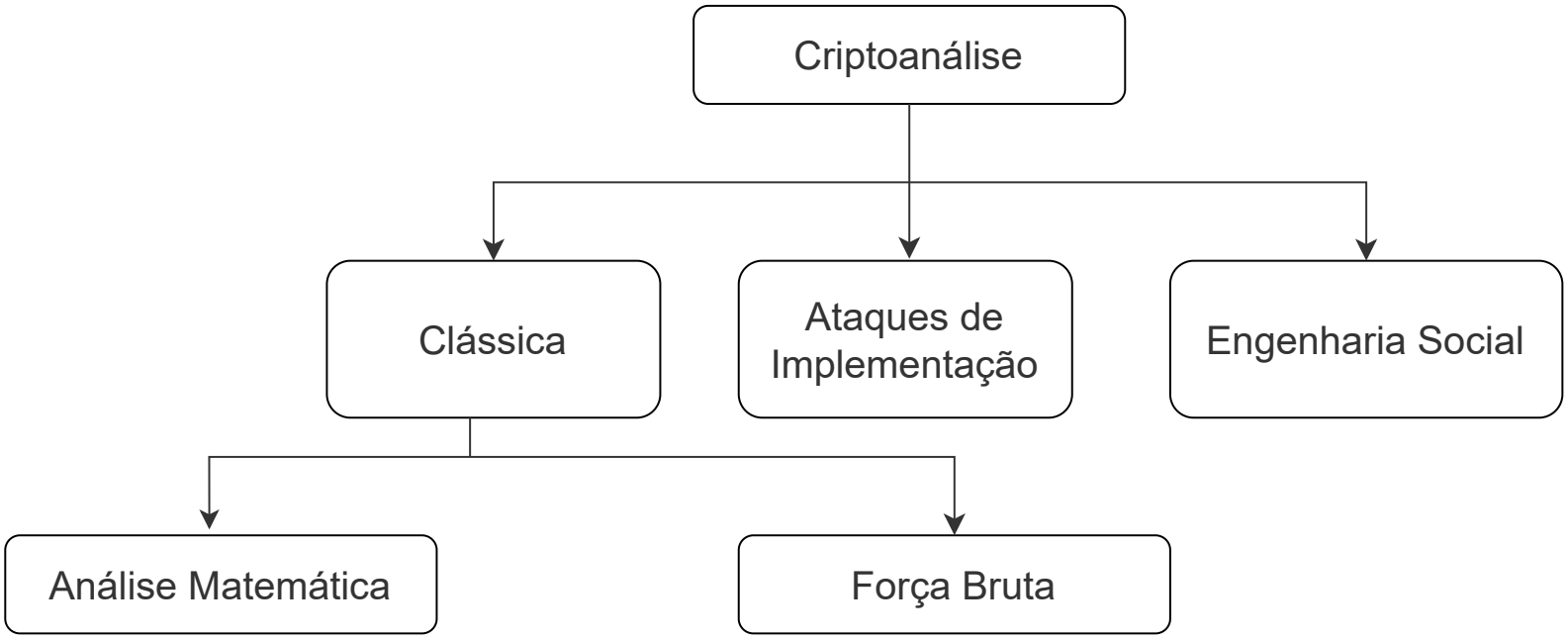
Força bruta

- Na prática, ataques de força bruta podem ser mais complicados por causa de chaves incorretas que podem dar falso positivos.
- Tecnicamente, sempre é possível usar um ataque de força bruta a um criptosistemas simétrico. Mas pode não ser possível na prática.
- Se a verificação de todas as chaves usando computadores modernos levar muitas décadas, dizemos que o sistema é `computacionalmente seguro` contra ataque de força bruta.

Frequência das letras na língua Português



Criptoanálise



Princípio de Kerckhoff - Definição

Um criptosistema deve ser seguro mesmo que o atacante conheça todos os detalhes do sistema, com exceção da chave.

Qual o Tamanho ideal da chave?

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

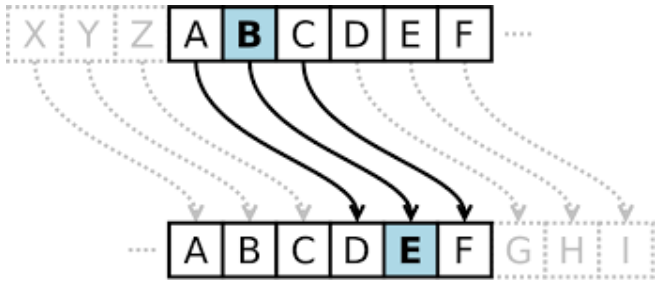
Date	Security Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
Legacy (1)	80	2TDEA	1024	160	1024	160	SHA-1 (2)	
2019 - 2030	112	(3TDEA) (3) AES-128	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2019 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128
2019 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
2019 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256

https://www.keylength.com/en/4/

Cifras Históricas

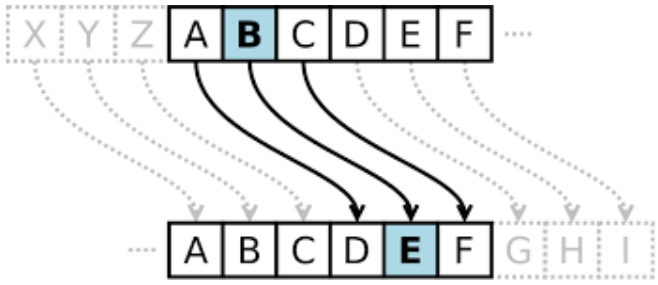
- Cifra de Cesar

Cifra de César



Cifra de César

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

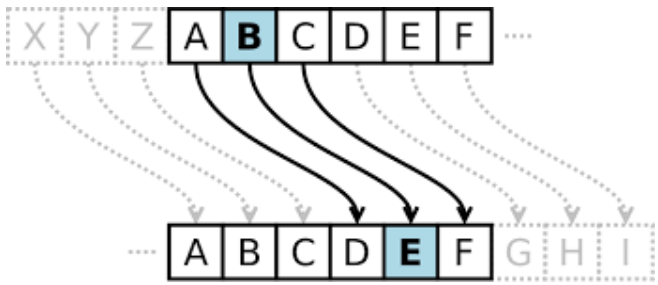


Definição

É uma cifra de bloco onde cada letra é representada por uma letra depois de k posições.

Cifra de César

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

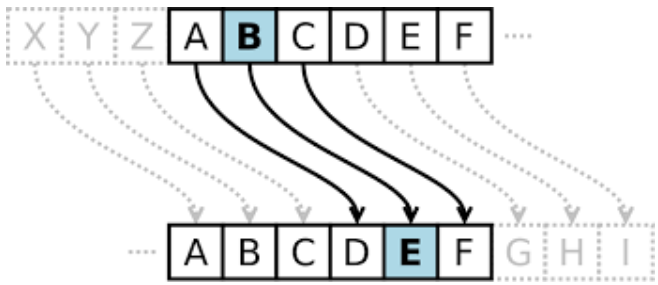


Definição

É uma cifra de bloco onde cada letra é representada por uma letra depois de k posições.

- Formalização:

Cifra de César

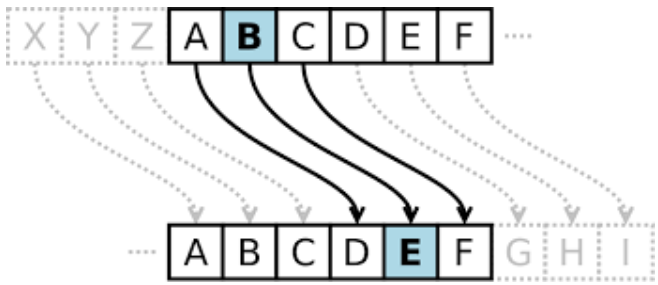


Definição

É uma cifra de bloco onde cada letra é representada por uma letra depois de k posições.

- Formalização:
  - Representa cada letra por um número x_i. A chave é o número k.

Cifra de César



Definição

É uma cifra de bloco onde cada letra é representada por uma letra depois de k posições.

- Formalização:
  - Representa cada letra por um número x_i. A chave é o número k.
  - A permutação é dada por $\pi(x_i) = (x_i + k) mod |\mathcal{A}|$.

Cifra de César

- Criptoanálise: busca exaustiva nas $|\mathcal{A}|$ chaves. Em média, testa apenas $\frac{|\mathcal{A}|}{2}$.

Cifra de César

- Criptoanálise: busca exaustiva nas $|\mathcal{A}|$ chaves. Em média, testa apenas $\frac{|\mathcal{A}|}{2}$.
- Propriedades desejáveis para uma cifra:

Cifra de César

- Criptoanálise: busca exaustiva nas $|\mathcal{A}|$ chaves. Em média, testa apenas $\frac{|\mathcal{A}|}{2}$.
- Propriedades desejáveis para uma cifra:
  - Espaço de chaves deve ser resistente à busca exaustiva de um atacante com poder computacional polinomial.

Polybius square

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Encriptação da mensagem “SEGREDO”: 43152242151434.

Cifra Afim

Definição

É um caso especial de substituição monoalfabética que aplica uma função linear.

$\text{Enc}_{k=(a,b)}(x) = (ax + b) \bmod m$.

$\text{Dec}_{k=(a,b)}(y) = a^{-1} \times (y - b) \bmod m$.

Cifra Afim

Definição

É um caso especial de substituição monoalfabética que aplica uma função linear.
$\text{Enc}_{k=(a,b)}(x) = (ax + b) \text{ mod } m$.
$\text{Dec}_{k=(a,b)}(y) = a^{-1} \times (y - b) \text{ mod } m$.

- Exemplo: para $m = 26 = 2 * 13$, os valores de a tal que mdc$(a, m) = 1$ são $\{1, 3, 5, 7, 9, 11, , 15, 17, 19, 21, 23, 25\}$

Cifra Afim

Definição

É um caso especial de substituição monoalfabética que aplica uma função linear.
$\text{Enc}_{k=(a,b)}(x) = (ax + b) \bmod m$.
$\text{Dec}_{k=(a,b)}(y) = a^{-1} \times (y - b) \bmod m$.

- Exemplo: para $m = 26 = 2 * 13$, os valores de a tal que mdc$(a, m) = 1$ são $\{1, 3, 5, 7, 9, 11, , 15, 17, 19, 21, 23, 25\}$
- O parâmetro b pode ser qualquer elemento de $\mathbb{Z}_m$. Nesse caso, a cifra afim tem apenas 12 * 26 chaves válidas.

Cifra de Transposição

Definição

A transposição $E_\theta : \mathcal{M} \to \mathcal{C}$ troca a i-ésima posição da letra m_i de uma mensagem m por $\theta(i)$, onde θ define a permutação do conjunto $\{1, 2, \ldots, |m|\}$.

Cifra de Transposição

Definição

A transposição $E_\theta : \mathcal{M} \to \mathcal{C}$ troca a i-ésima posição da letra m_i de uma mensagem m por $\theta(i)$, onde θ define a permutação do conjunto $\{1, 2, \ldots, |m|\}$.

- Em outras palavras?

Cifra de Transposição

Definição

A transposição $E_\theta : \mathcal{M} \to \mathcal{C}$ troca a i-ésima posição da letra m_i de uma mensagem m por $\theta(i)$, onde θ define a permutação do conjunto $\{1, 2, \ldots, |m|\}$.

- Em outras palavras?
  - A chave da permutação $\theta : \{1, 2, \ldots, |m|\} \to \{1, 2, \ldots, |m|\}$.

Cifra de Transposição

Definição

A transposição $E_\theta : \mathcal{M} \to \mathcal{C}$ troca a i-ésima posição da letra m_i de uma mensagem m por $\theta(i)$, onde θ define a permutação do conjunto $\{1, 2, \ldots, |m|\}$.

- Em outras palavras?
  - A chave da permutação $\theta : \{1, 2, \ldots, |m|\} \to \{1, 2, \ldots, |m|\}$.
  - A função de encriptação é $E_\theta(m) = (m_{\theta_1}, m_{\theta_2}, \ldots, m_{\theta_{|m|}})$.

Cifra de Transposição

Definição

A transposição $E_\theta : \mathcal{M} \to \mathcal{C}$ troca a i-ésima posição da letra m_i de uma mensagem m por $\theta(i)$, onde θ define a permutação do conjunto $\{1, 2, \ldots, |m|\}$.

- Em outras palavras?
  - A chave da permutação $\theta : \{1, 2, \ldots, |m|\} \to \{1, 2, \ldots, |m|\}$.
  - A função de encriptação é $E_\theta(m) = (m_{\theta_1}, m_{\theta_2}, \ldots, m_{\theta_{|m|}})$.
  - A função de dencriptação é $D_\theta(c) = (c_{\theta_1}^{-1}, c_{\theta_2}^{-1}, \ldots, c_{\theta_{|m|}}^{-1})$.

Cifra de Transposição

Definição

A transposição $E_\theta : \mathcal{M} \to \mathcal{C}$ troca a i-ésima posição da letra m_i de uma mensagem m por $\theta(i)$, onde θ define a permutação do conjunto $\{1, 2, \ldots, |m|\}$.

- Em outras palavras?
  - A chave da permutação $\theta : \{1, 2, \ldots, |m|\} \to \{1, 2, \ldots, |m|\}$.
  - A função de encriptação é $E_\theta(m) = (m_{\theta_1}, m_{\theta_2}, \ldots, m_{\theta_{|m|}})$.
  - A função de dencriptação é $D_\theta(c) = (c_{\theta_1}^{-1}, c_{\theta_2}^{-1}, \ldots, c_{\theta_{|m|}}^{-1})$.
- Observações:

Cifra de Transposição

Definição

A transposição $E_\theta : \mathcal{M} \to \mathcal{C}$ troca a i-ésima posição da letra m_i de uma mensagem m por $\theta(i)$, onde θ define a permutação do conjunto $\{1, 2, \ldots, |m|\}$.

- Em outras palavras?
  - A chave da permutação $\theta : \{1, 2, \ldots, |m|\} \to \{1, 2, \ldots, |m|\}$.
  - A função de encriptação é $E_\theta(m) = (m_{\theta_1}, m_{\theta_2}, \ldots, m_{\theta_{|m|}})$.
  - A função de dencriptação é $D_\theta(c) = (c_{\theta_1}^{-1}, c_{\theta_2}^{-1}, \ldots, c_{\theta_{|m|}}^{-1})$.
- Observações:
  - O espaço de chaves possui tamanho $(|m|!)$.

Cifra de Transposição

Definição

A transposição $E_\theta : \mathcal{M} \to \mathcal{C}$ troca a i-ésima posição da letra m_i de uma mensagem m por $\theta(i)$, onde θ define a permutação do conjunto $\{1, 2, \ldots, |m|\}$.

- Em outras palavras?
  - A chave da permutação $\theta : \{1, 2, \ldots, |m|\} \to \{1, 2, \ldots, |m|\}$.
  - A função de encriptação é $E_\theta(m) = (m_{\theta_1}, m_{\theta_2}, \ldots, m_{\theta_{|m|}})$.
  - A função de dencriptação é $D_\theta(c) = (c_{\theta_1}^{-1}, c_{\theta_2}^{-1}, \ldots, c_{\theta_{|m|}}^{-1})$.
- Observações:
  - O espaço de chaves possui tamanho $(|m|!)$.
  - No caso geral, a chave possui tamanho $|m|$.

Scytale (Sparta, 500 A.C)

Cifras de substituição Homofônicas

Definição

Uma substituição homofônica mapeia cada caractere m_i de uma mensagem m por uma das letras do conjunto $H(m_i)$.

Cifras de substituição Homofônicas

Definição

Uma substituição homofônica mapeia cada caractere m_i de uma mensagem m por uma das letras do conjunto $H(m_i)$.

- Observações:

Cifras de substituição Homofônicas

Definição

Uma substituição homofônica mapeia cada caractere m_i de uma mensagem m por uma das letras do conjunto $H(m_i)$.

- Observações:
  - O alfabeto de definições deve ser estendido com os novos símbolos.

Cifras de substituição Homofônicas

Definição

Uma substituição homofônica mapeia cada caractere m_i de uma mensagem m por uma das letras do conjunto $H(m_i)$.

- Observações:
  - O alfabeto de definições deve ser estendido com os novos símbolos.
  - A criptoanálise é mais difícil, mas as relações entre os símbolos permanecem.

Cifras de substituição Homofônicas

Definição

Uma substituição homofônica mapeia cada caractere m_i de uma mensagem m por uma das letras do conjunto $H(m_i)$.

- Observações:
  - O alfabeto de definições deve ser estendido com os novos símbolos.
  - A criptoanálise é mais difícil, mas as relações entre os símbolos permanecem.
  - Vulnerável contra a análise de frequência de bigramas e trigramas.

Cifra de substituição polialfabética

Definição

Uma substituição polialfabética mapeia conjuntos disjuntos de caracteres com permutações π_i distintas.

Cifra de substituição polialfabética

Definição

Uma substituição polialfabética mapeia conjuntos disjuntos de caracteres com permutações π_i distintas.

- Ou seja:

Cifra de substituição polialfabética

Definição

Uma substituição polialfabética mapeia conjuntos disjuntos de caracteres com permutações π_i distintas.

- Ou seja:
  - A chave é o conjunto de permutações $\Pi = \pi_1, \pi_2, \ldots, \pi_t$.

Cifra de substituição polialfabética

Definição

Uma substituição polialfabética mapeia conjuntos disjuntos de caracteres com permutações π_i distintas.

- Ou seja:
  - A chave é o conjunto de permutações $\Pi = \pi_1, \pi_2, \ldots, \pi_t$.
  - A função de encriptação é $E_\Pi(m) = (\pi_1(m_1), \pi_2(m_2), \ldots, \pi_t(m_t))$.

Cifra de substituição polialfabética

Definição

Uma substituição polialfabética mapeia conjuntos disjuntos de caracteres com permutações π_i distintas.

- Ou seja:
  - A chave é o conjunto de permutações $\Pi = \pi_1, \pi_2, \ldots, \pi_t$.
  - A função de encriptação é $E_\Pi(m) = (\pi_1(m_1), \pi_2(m_2), \ldots, \pi_t(m_t))$.
  - A função de decriptação é análoga.

Cifra de substituição polialfabética

Definição

Uma substituição polialfabética mapeia conjuntos disjuntos de caracteres com permutações π_i distintas.

- Ou seja:
  - A chave é o conjunto de permutações $\Pi = \pi_1, \pi_2, \ldots, \pi_t$.
  - A função de encriptação é $E_\Pi(m) = (\pi_1(m_1), \pi_2(m_2), \ldots, \pi_t(m_t))$.
  - A função de decriptação é análoga.
- Observações:

Cifra de substituição polialfabética

Definição

Uma substituição polialfabética mapeia conjuntos disjuntos de caracteres com permutações π_i distintas.

- Ou seja:
  - A chave é o conjunto de permutações $\Pi = \pi_1, \pi_2, \ldots, \pi_t$.
  - A função de encriptação é $E_\Pi(m) = (\pi_1(m_1), \pi_2(m_2), \ldots, \pi_t(m_t))$.
  - A função de decriptação é análoga.
- Observações:
  - A frequência do símbolos é distorcida!

Cifra de deslocamento polialfabética (Vigenère)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Definição

A cifra de deslocamento polialfabética é um caso especial de uma cifra de substituição polialfabética onde cada permutação é uma cifra de deslocamento elementar.

Cifra de deslocamento polialfabética (Vigenère)

Definição

A cifra de deslocamento polialfabética é um caso especial de uma cifra de substituição polialfabética onde cada permutação é uma cifra de deslocamento elementar.

- Formalização (assumir aritmética módulo m):

Cifra de deslocamento polialfabética (Vigenère)

Definição

A cifra de deslocamento polialfabética é um caso especial de uma cifra de substituição polialfabética onde cada permutação é uma cifra de deslocamento elementar.

- Formalização (assumir aritmética módulo m):
  - Defina $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^t$

Cifra de deslocamento polialfabética (Vigenère)

Definição

A cifra de deslocamento polialfabética é um caso especial de uma cifra de substituição polialfabética onde cada permutação é uma cifra de deslocamento elementar.

- Formalização (assumir aritmética módulo m):
  - Defina $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^t$
  - A chave é o conjunto $K = k_1, k_2, \ldots, k_t$.

Cifra de deslocamento polialfabética (Vigenère)

Definição

A cifra de deslocamento polialfabética é um caso especial de uma cifra de substituição polialfabética onde cada permutação é uma cifra de deslocamento elementar.

- Formalização (assumir aritmética módulo m):
  - Defina $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^t$
  - A chave é o conjunto $K = k_1, k_2, \ldots, k_t$.
  - A função de encriptação é
    $y = Enc_k(x) = (x_1 + k_1, x_2 + k_2, \ldots, x_t + k_t)$.

Cifra de deslocamento polialfabética (Vigenère)

Definição

A cifra de deslocamento polialfabética é um caso especial de uma cifra de substituição polialfabética onde cada permutação é uma cifra de deslocamento elementar.

- Formalização (assumir aritmética módulo m):
  - Defina $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^t$
  - A chave é o conjunto $K = k_1, k_2, \ldots, k_t$.
  - A função de encriptação é
    $y = Enc_k(x) = (x_1 + k_1, x_2 + k_2, \ldots, x_t + k_t)$.
  - A função de decriptação é
    $x = Dec_k(y) = (y_1 - k_1, y_2 - k_2, \ldots, y_t - k_t)$..

Cifra de deslocamento polialfabética (Vigenère)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Definição

A cifra de deslocamento polialfabética é um caso especial de uma cifra de substituição polialfabética onde cada permutação é uma cifra de deslocamento elementar.

- Formalização (assumir aritmética módulo m):
  - Defina $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^t$
  - A chave é o conjunto $K = k_1, k_2, \ldots, k_t$.
  - A função de encriptação é
    $y = Enc_k(x) = (x_1 + k_1, x_2 + k_2, \ldots, x_t + k_t)$.
  - A função de decriptação é
    $x = Dec_k(y) = (y_1 - k_1, y_2 - k_2, \ldots, y_t - k_t)$..
  - Qual o número possível de chaves?

Cifra de deslocamento polialfabética (Vigenère)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Definição

A cifra de deslocamento polialfabética é um caso especial de uma cifra de substituição polialfabética onde cada permutação é uma cifra de deslocamento elementar.

- Formalização (assumir aritmética módulo m):
  - Defina $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^t$
  - A chave é o conjunto $K = k_1, k_2, \ldots, k_t$.
  - A função de encriptação é
    $y = Enc_k(x) = (x_1 + k_1, x_2 + k_2, \ldots, x_t + k_t)$.
  - A função de decriptação é
    $x = Dec_k(y) = (y_1 - k_1, y_2 - k_2, \ldots, y_t - k_t)$..
  - Qual o número possível de chaves?
  - O espaço de chaves é m^t.

Cifra de Vigenère

Ficou conhecida como “le chiffre indéchiffrable”, pois ficou indecifrável por quase 300 anos!

	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

Cifra de Vigenère

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Usando a cifra de Vigenère com a chave “UFCQUIXADA”, faça a encriptação do seu nome completo.

Criptoanálise

- Cifra de deslocamento: busca exaustiva em $\mathcal{K}$;

Criptoanálise

- Cifra de deslocamento: busca exaustiva em $\mathcal{K}$;
- Cifra de substituição monoalfabética: análise de frequência;

Criptoanálise

- Cifra de deslocamento: busca exaustiva em $\mathcal{K}$;
- Cifra de substituição monoalfabética: análise de frequência;
- Cifra afim: análise de frequência e sistema linear de equações;

Criptoanálise

- Cifra de deslocamento: busca exaustiva em $\mathcal{K}$;
- Cifra de substituição monoalfabética: análise de frequência;
- Cifra afim: análise de frequência e sistema linear de equações;
- Cifra de transposição: solução de anagrama, ataque de texto claro conhecido;

Criptoanálise

- Cifra de deslocamento: busca exaustiva em $\mathcal{K}$;
- Cifra de substituição monoalfabética: análise de frequência;
- Cifra afim: análise de frequência e sistema linear de equações;
- Cifra de transposição: solução de anagrama, ataque de texto claro conhecido;
- Cifra de substituição polialfabética: partição e análise de frequência;

Criptoanálise

- Cifra de deslocamento: busca exaustiva em $\mathcal{K}$;
- Cifra de substituição monoalfabética: análise de frequência;
- Cifra afim: análise de frequência e sistema linear de equações;
- Cifra de transposição: solução de anagrama, ataque de texto claro conhecido;
- Cifra de substituição polialfabética: partição e análise de frequência;
- Cifra de deslocamento polialfabética: índice de coincidências e análise de frequência;

Criptoanálise

- Cifra de deslocamento: busca exaustiva em $\mathcal{K}$;
- Cifra de substituição monoalfabética: análise de frequência;
- Cifra afim: análise de frequência e sistema linear de equações;
- Cifra de transposição: solução de anagrama, ataque de texto claro conhecido;
- Cifra de substituição polialfabética: partição e análise de frequência;
- Cifra de deslocamento polialfabética: índice de coincidências e análise de frequência;
- Cifra de Hill: ataque de texto claro conhecido.

Cifra ADFGVX (Nebel 1918)

- Aplica substituição seguida de uma transposição!

Cifra ADFGVX (Nebel 1918)

- Aplica substituição seguida de uma transposição!
- O primeiro passo é substituir as letras da mensagem original pelas letras equivalentes em um quadrado de Pólibio.

	A	**D**	**F**	**G**	**V**	**X**
A	N	1	H	D	Z	3
D	4	C	T	5	I	Y
F	7	E	6	2	Q	8
G	8	K	U	A	O	F
V	R	M	0	S	V	W
X	P	L	J	X	B	G

Cifra ADFGVX (Nebel 1918)

- Aplica substituição seguida de uma transposição!
- O primeiro passo é substituir as letras da mensagem original pelas letras equivalentes em um quadrado de Pólibio.

	A	**D**	**F**	**G**	**V**	**X**
A	N	1	H	D	Z	3
D	4	C	T	5	I	Y
F	7	E	6	2	Q	8
G	8	K	U	A	O	F
V	R	M	0	S	V	W
X	P	L	J	X	B	G

- Mensagem Original: E R I C C A B R A L

Cifra ADFGVX (Nebel 1918)

- Aplica substituição seguida de uma transposição!
- O primeiro passo é substituir as letras da mensagem original pelas letras equivalentes em um quadrado de Pólibio.

	A	**D**	**F**	**G**	**V**	**X**
A	N	1	H	D	Z	3
D	4	C	T	5	I	Y
F	7	E	6	2	Q	8
G	8	K	U	A	O	F
V	R	M	0	S	V	W
X	P	L	J	X	B	G

- Mensagem Original: E R I C C A B R A L
- Mensagem Cifrada: FD VA DV DD DD GG XV VA GG XD

Cifra ADFGVX (Nebel 1918)

- A mensagem é então organizada em uma tabela baseada numa chave de tamanho variável de acordo com a dimensão da mensagem. Suponha que a chave é a palavra FATO.

F	**A**	**T**	**O**
F	D	V	A
D	V	D	D
D	D	G	G
X	V	V	A
G	G	X	D

Cifra ADFGVX (Nebel 1918)

- A mensagem é então organizada em uma tabela baseada numa chave de tamanho variável de acordo com a dimensão da mensagem. Suponha que a chave é a palavra FATO.

F	**A**	**T**	**O**
F	D	V	A
D	V	D	D
D	D	G	G
X	V	V	A
G	G	X	D

Cifra ADFGVX (Nebel 1918)

- A mensagem é então organizada em uma tabela baseada numa chave de tamanho variável de acordo com a dimensão da mensagem. Suponha que a chave é a palavra FATO.

F	**A**	**T**	**O**
F	D	V	A
D	V	D	D
D	D	G	G
X	V	V	A
G	G	X	D

$\rightarrow$

A	**F**	**O**	**T**
D	F	A	V
V	D	D	D
D	D	G	G
V	X	A	V
G	G	D	X

- Cifra final: DFAV VDDD DDGG VXAV GGDX

Máquina Enigma (Scherbius, 1928)

- Peça fundamental na estratégia de Hitler. O Enigma é uma máquina eletromecânica de criptografia com rotores.

Máquina Enigma - Funcionamento

- A Máquina Enigma é uma combinação de sistemas mecânicos e elétricos.

Máquina Enigma - Funcionamento

- A Máquina Enigma é uma combinação de sistemas mecânicos e elétricos.
- O mecanismo consiste num teclado, em um conjunto de rotores, dispostos em fila e de um mecanismo de avanço que faz andar alguns rotores uma posição quando uma tecla é pressionada.

Máquina Enigma - Funcionamento

- A Máquina Enigma é uma combinação de sistemas mecânicos e elétricos.
- O mecanismo consiste num teclado, em um conjunto de rotores, dispostos em fila e de um mecanismo de avanço que faz andar alguns rotores uma posição quando uma tecla é pressionada.
- Espaço de chaves;

Máquina Enigma - Funcionamento

- A Máquina Enigma é uma combinação de sistemas mecânicos e elétricos.
- O mecanismo consiste num teclado, em um conjunto de rotores, dispostos em fila e de um mecanismo de avanço que faz andar alguns rotores uma posição quando uma tecla é pressionada.
- Espaço de chaves;
  - Cada rotor tinha 26 orientações diferentes.

Máquina Enigma - Funcionamento

- A Máquina Enigma é uma combinação de sistemas mecânicos e elétricos.
- O mecanismo consiste num teclado, em um conjunto de rotores, dispostos em fila e de um mecanismo de avanço que faz andar alguns rotores uma posição quando uma tecla é pressionada.
- Espaço de chaves;
  - Cada rotor tinha 26 orientações diferentes.
  - Eles podiam ser dispostos em seis diferentes combinações.

Máquina Enigma - Funcionamento

- A Máquina Enigma é uma combinação de sistemas mecânicos e elétricos.
- O mecanismo consiste num teclado, em um conjunto de rotores, dispostos em fila e de um mecanismo de avanço que faz andar alguns rotores uma posição quando uma tecla é pressionada.
- Espaço de chaves;
  - Cada rotor tinha 26 orientações diferentes.
  - Eles podiam ser dispostos em seis diferentes combinações.
  - No total, mais de 10^6 chaves eram possíveis.

Máquina Enigma - Funcionamento

- A Máquina Enigma é uma combinação de sistemas mecânicos e elétricos.
- O mecanismo consiste num teclado, em um conjunto de rotores, dispostos em fila e de um mecanismo de avanço que faz andar alguns rotores uma posição quando uma tecla é pressionada.
- Espaço de chaves;
  - Cada rotor tinha 26 orientações diferentes.
  - Eles podiam ser dispostos em seis diferentes combinações.
  - No total, mais de 10^6 chaves eram possíveis.
- Os operadores de máquinas usaram chaves diárias de um livro de códigos e chaves efêmeras criptografadas no início de cada mensagem.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- O trabalho criptoanalítico foi iniciado pelo polonês (Rejewski):

Máquina Enigma - Criptoanálise (Rejewski, 1928)

- O trabalho criptoanalítico foi iniciado pelo polonês (Rejewski):
  - Manual de operação roubado da inteligência alemã.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

- O trabalho criptoanalítico foi iniciado pelo polonês (Rejewski):
  - Manual de operação roubado da inteligência alemã.
  - A chave efêmera (configuração da máquina) foi repetida.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

- O trabalho criptoanalítico foi iniciado pelo polonês (Rejewski):
  - Manual de operação roubado da inteligência alemã.
  - A chave efêmera (configuração da máquina) foi repetida.
  - As chaves efêmeras vazavam relações entre letras.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

- O trabalho criptoanalítico foi iniciado pelo polonês (Rejewski):
  - Manual de operação roubado da inteligência alemã.
  - A chave efêmera (configuração da máquina) foi repetida.
  - As chaves efêmeras vazavam relações entre letras.
  - Uma vez que esta é uma cifra polialfabética, as relações eram periódicas.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- O trabalho criptoanalítico foi iniciado pelo polonês (Rejewski):
  - Manual de operação roubado da inteligência alemã.
  - A chave efêmera (configuração da máquina) foi repetida.
  - As chaves efêmeras vazavam relações entre letras.
  - Uma vez que esta é uma cifra polialfabética, as relações eram periódicas.
- O espaço de chaves foi reduzido para 105456 configurações dos rotores.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

- Rejewski passou 1 ano construindo um catálogo de períodos. Sua rotina diária era:

Máquina Enigma - Criptoanálise (Rejewski, 1928)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Rejewski passou 1 ano construindo um catálogo de períodos. Sua rotina diária era:
  - Receber as primeiras 6 mensagens do dia.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Rejewski passou 1 ano construindo um catálogo de períodos. Sua rotina diária era:
  - Receber as primeiras 6 mensagens do dia.
  - Computar as relações de período.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Rejewski passou 1 ano construindo um catálogo de períodos. Sua rotina diária era:
  - Receber as primeiras 6 mensagens do dia.
  - Computar as relações de período.
  - Verificar o catálogo das configurações de rotores.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Rejewski passou 1 ano construindo um catálogo de períodos. Sua rotina diária era:
  - Receber as primeiras 6 mensagens do dia.
  - Computar as relações de período.
  - Verificar o catálogo das configurações de rotores.
  - Resolver as substituições aplicadas ao painel.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

- Rejewski passou 1 ano construindo um catálogo de períodos. Sua rotina diária era:
  - Receber as primeiras 6 mensagens do dia.
  - Computar as relações de período.
  - Verificar o catálogo das configurações de rotores.
  - Resolver as substituições aplicadas ao painel.
- Eventualmente, Rejewski atualizou seis enigmas para automatizar o processo.

Máquina Enigma - Criptoanálise (Rejewski, 1928)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Rejewski passou 1 ano construindo um catálogo de períodos. Sua rotina diária era:
  - Receber as primeiras 6 mensagens do dia.
  - Computar as relações de período.
  - Verificar o catálogo das configurações de rotores.
  - Resolver as substituições aplicadas ao painel.
- Eventualmente, Rejewski atualizou seis enigmas para automatizar o processo.
- Rejewski conseguiu transferir seu método para os ingleses apenas duas semanas antes da Polônia ser invadida.

Máquina Enigma (Scherbius, 1928)

- Nova versão da máquina:

Máquina Enigma (Scherbius, 1928)

- Nova versão da máquina:
  - Dois novos rotores;

Máquina Enigma (Scherbius, 1928)

- Nova versão da máquina:
  - Dois novos rotores;
  - Os rotores podiam ser dispostos em 60 combinações diferentes;

Máquina Enigma (Scherbius, 1928)

- Nova versão da máquina:
  - Dois novos rotores;
  - Os rotores podiam ser dispostos em 60 combinações diferentes;
  - O painel de substituição permitia a troca de 10 letras.

Máquina Enigma (Scherbius, 1928)

- Nova versão da máquina:
  - Dois novos rotores;
  - Os rotores podiam ser dispostos em 60 combinações diferentes;
  - O painel de substituição permitia a troca de 10 letras.
  - No total, mais de 10^{20} chaves eram possíveis.

Máquina Enigma - Criptoanálise (Turing, 1940)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- O trabalho na criptoanálise continuou em Bletchley Park.

Máquina Enigma - Criptoanálise (Turing, 1940)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- O trabalho na criptoanálise continuou em Bletchley Park.
- O esforço inicial consistiu no uso de restrições operacionais para acelerar o ataque Polonês.

Máquina Enigma - Criptoanálise (Turing, 1940)

- O trabalho na criptoanálise continuou em Bletchley Park.
- O esforço inicial consistiu no uso de restrições operacionais para acelerar o ataque Polonês.
- Mas um dia, os alemãs pararam de repetir a chave efêmera.

Máquina Enigma - Criptoanálise (Turing, 1940)

- O trabalho na criptoanálise continuou em Bletchley Park.
- O esforço inicial consistiu no uso de restrições operacionais para acelerar o ataque Polonês.
- Mas um dia, os alemãs pararam de repetir a chave efêmera.
- Alan Turing foi responsável por quebrar ENIGMA novamente.

Máquina Enigma - Criptoanálise (Turing, 1940)

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Turing observou que:

Máquina Enigma - Criptoanálise (Turing, 1940)

- Turing observou que:
  - A palavra alemão “wetter” sempre aparecia na mesma posição.

Máquina Enigma - Criptoanálise (Turing, 1940)

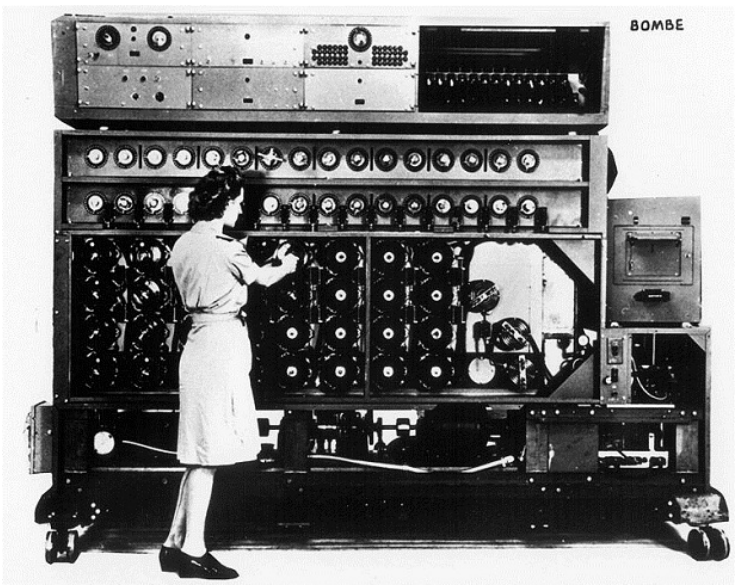
- Turing observou que:
  - A palavra alemão “wetter” sempre aparecia na mesma posição.
  - Esta palavra definiu novas relações periódicas.

Máquina Enigma - Criptoanálise (Turing, 1940)

- Turing observou que:
  - A palavra alemão “wetter” sempre aparecia na mesma posição.
  - Esta palavra definiu novas relações periódicas.
  - Os períodos foram novamente diferentes do painel.

Máquina Enigma - Criptoanálise (Turing, 1940)

- Turing observou que:
  - A palavra alemão “wetter” sempre aparecia na mesma posição.
  - Esta palavra definiu novas relações periódicas.
  - Os períodos foram novamente diferentes do painel.
  - Uma máquina poderia ser construída para exercer as configurações restantes do rotor!



Curiosidades

- Os aliados usaram Navajos e sua língua como mecanismo de encriptação.

Curiosidades

- Os aliados usaram Navajos e sua língua como mecanismo de encriptação.
- Os ingleses falharam algumas vezes para esconder o fato de terem quebrado o enigma.

Curiosidades

- Os aliados usaram Navajos e sua língua como mecanismo de encriptação.
- Os ingleses falharam algumas vezes para esconder o fato de terem quebrado o enigma.
- Criptoanalistas foram recrutados por meio de palavras cruzadas no jornal.

Referências

- Understanding Cryptography: A Textbook for Students and Practitioners (Paar and Pelzl);
- Handbook of Applied Cryptography (Menezes et al.);
- The Code Book (Singh)
- http://www.clubedosgenerais.org/site/artigos/57/2014/06/enigma/
- Slides da disciplina MO421 da UNICAMP (professor Diego Aranha).

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

FIM