Prime

Conceitos de Criptografia

Confusão, Difusão e Ofuscação

Confusão - Princípio de garantir que a relação entre a chave de criptografia e os dados depois de criptografados seja a mais complexa possível.

Difusão - Garantia de que a repetição de caracteres no texto simples não facilite a decifrar o texto cifrado.

Ofuscação - Conceito de tornar algo complicado de propósito para torná-lo difícil de entender.

O que é e Por que Usamos Criptografia?

- CIANA é a palavra de ordem na Criptografia.
- A "escrita secreta" existe desde os primórdios.
  - Manter o conteúdo em segredo e autêntico;
  - E que o segredo seja transmitido com segurança.
- Recursos da criptografia:
  - Confidencialidade;
  - Utilidade;
  - Exclusividade;
  - Identidade;
  - Privacidade;
  - Não repúdio;
  - Integridade;
  - Segurança.

Definições

- Usa substituição e/ou transposição para se tornar oculto.
- Substituição e transposição dependem de várias etapas.
- Criptografia clássica - Elementos de linguagens naturais.
- Criptografia moderna - Conceitos avançados de matemática.
- O significado original é sempre devolvido a nós.
- **Criptografia:** Arte e ciência de transformar informações de texto simples através de técnicas de criptografias em texto cifrado, podendo ser descriptografado.

Criptografia, Criptologia ou...?

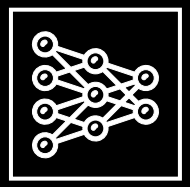
- Criptografia e criptologia não são a mesma coisa!
  - Criptografia – Uso e prática de técnicas criptográficas.
  - Criptoanálise - Estudo de vulnerabilidades em algoritmos e sistemas criptográficos.
  - Criptologia – Estudo combinado da criptografia e criptoanálise.
  - Criptolinguística - Tradução entre línguas humanas para produzir informações úteis.
- Criptogramas (jogos) não fazem parte desse campo!

Entendendo a Criptografia

O serviço de criptografia oferece mais do que apenas a encriptação, como: **criptografia**, **hash** e **autenticação**.

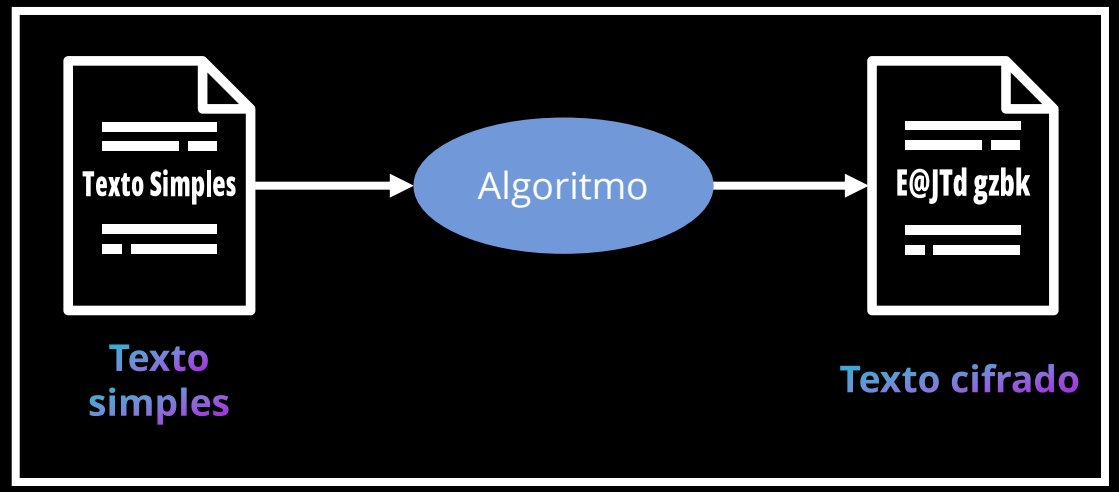
Plain text (texto simples) é a informação em um formato legível.

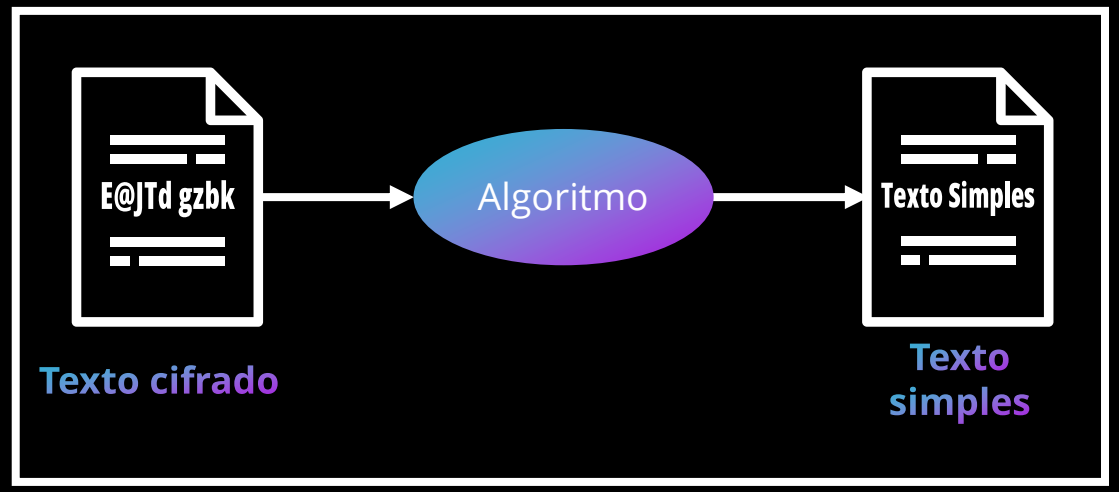
Cipher text (texto cifrado) é a informação em um formato criptografado e ilegível.



Para criptografar e descriptografar, usamos algoritmo de criptografia.

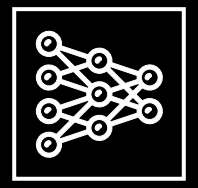
Convertendo Texto em Cifras





Componentes da Criptografia

Autenticação - Fornecem um método para provar que o remetente e o criador da informação são quem eles dizem ser.



Algoritmo - Operação matemática com os dados para converter os dados de texto simples em texto cifrado.

Chave - Informação variável para realizar a criptografia/descriptografia.

Autenticação

Qualquer solicitação de acesso ou uso de ativo de informação precisa ser autenticada.

Necessidade de envio das credenciais.

Informações de credenciamento devem ser armazenadas por assuntos e sistemas.

Não há necessidade de descriptografar para validar as credenciais.

Força da Chave

- A força da criptografia depende da força da chave.
- Quanto maior a chave, maior a entropia (força).
- Quanto maior a chave, mais tempo para processar.
- Exemplo mínimos de **Comprimentos:**

Chave simétrica de pelo menos 80 a 112 bits.

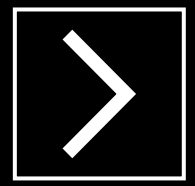
Chave de curva elíptica de pelo menos 160 a 224 bits.

Chave RSA ou EV da CA/Browser de pelo menos 2048 bits.

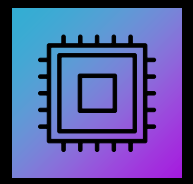
Chave DSA de pelo menos 2048 bits.

Alongamento das Chaves

Alongar ou fortalecer uma chave pode combater ataques de força bruta, como Argon2, Scrypt, PBKDF2 e Bcrypt.



Alongar é “esticar” uma chave fraca. eliminando a possibilidade de fácil adivinhação.



Para transformar uma chave mais forte, amenta o *keyspace*, consequentemente, o processamento.

O alongamento de chave envolve aumentar a complexidade computacional, amentando a carga de trabalho da força bruta.

Usando a Cifra de César

Incrementar cada caractere na mensagem por <key>.

O objetivo da chave é garantir que, se alguém descobrir o algoritmo, não será capaz de descriptografá-la.

A cifra de César não é um algoritmo forte para usar hoje.

Problema:

- Facilmente quebrada por conta de padrões linguísticos na linguagem.

Cifras de Substituição

- Cifra de substituição:

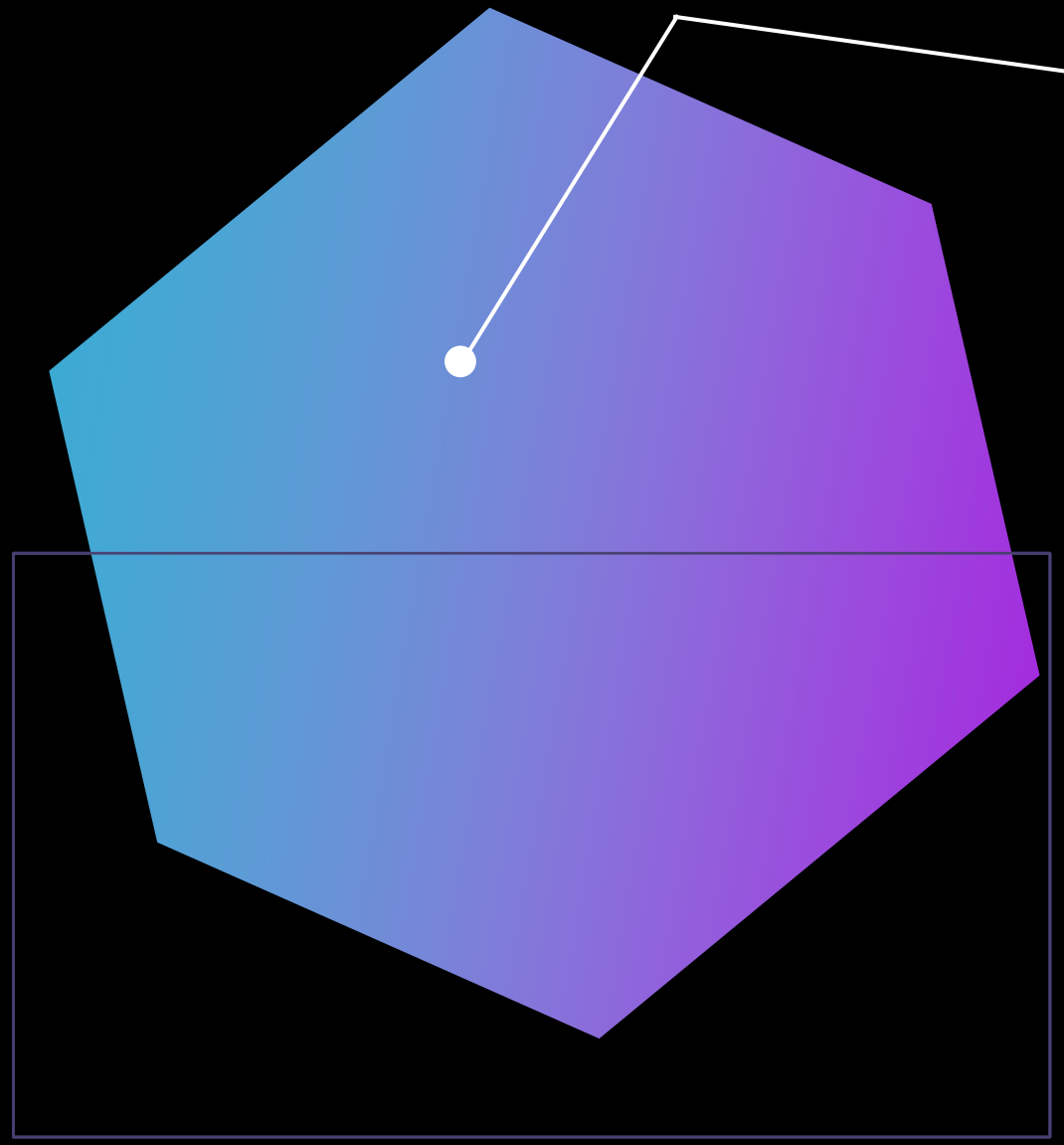
Texto simples: `O tio Adriano foi muito legal`

Texto cifrado: `P ujp Besjbop gpj nvjup mfhbm`

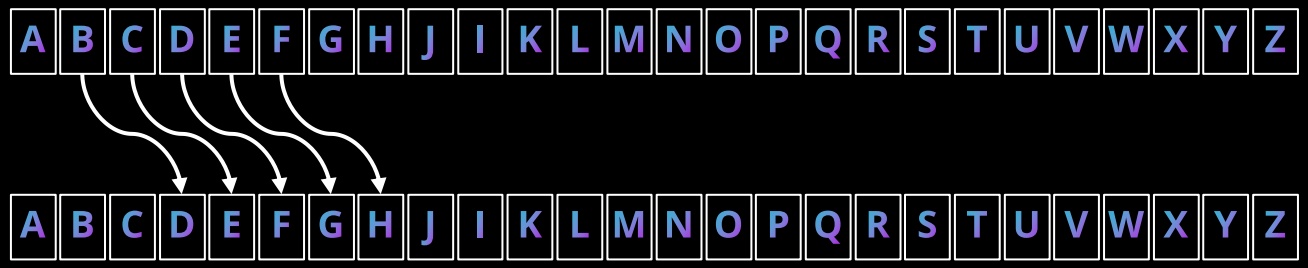
Texto simples: `O tio Adriano foi muito legal`

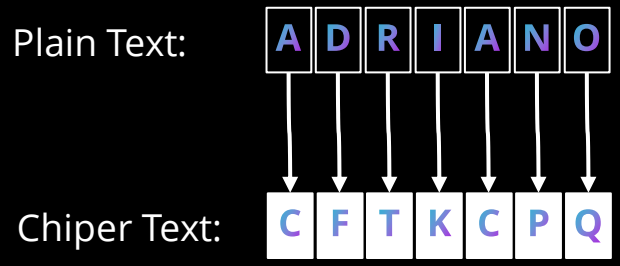
Cifra de César: `R xlr Dguldqr iRl pzlxr ohjdo`

Cifra ROT13: `B gvb Nqevnab sbv zhvgb yrtny`



Exemplo de Cifragem





- **Algoritmo:** Substituição
- **Chave:** 2

Chaves com Palavras

- Exemplo:

Mensagem: `canaldahora`

Chave: `assineagora`

1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M
14	**15**	**16**	**17**	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Mensagem:	**3**	**1**	**14**	**3**	**12**	**4**	**1**	**8**	**15**	**18**	**1**
Chave:	**1**	**19**	**19**	**9**	**14**	**5**	**1**	**7**	**15**	**18**	**1**
Total:	**4**	**20**	**7**	**12**	**26**	**9**	**2**	**15**	**4**	**10**	**2**
Cifra:	D	T	G	L	Z	I	B	O	D	J	B

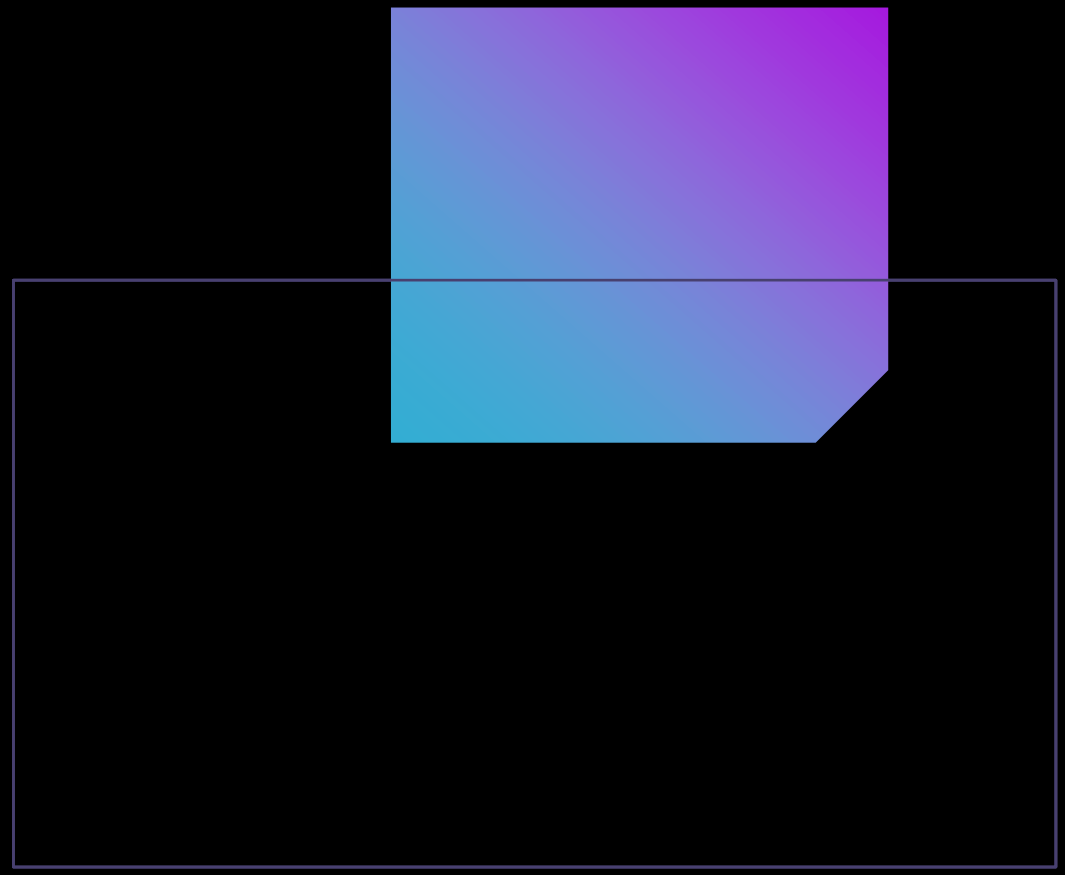
Cifra de Transposição

- Cifra de Transposição:

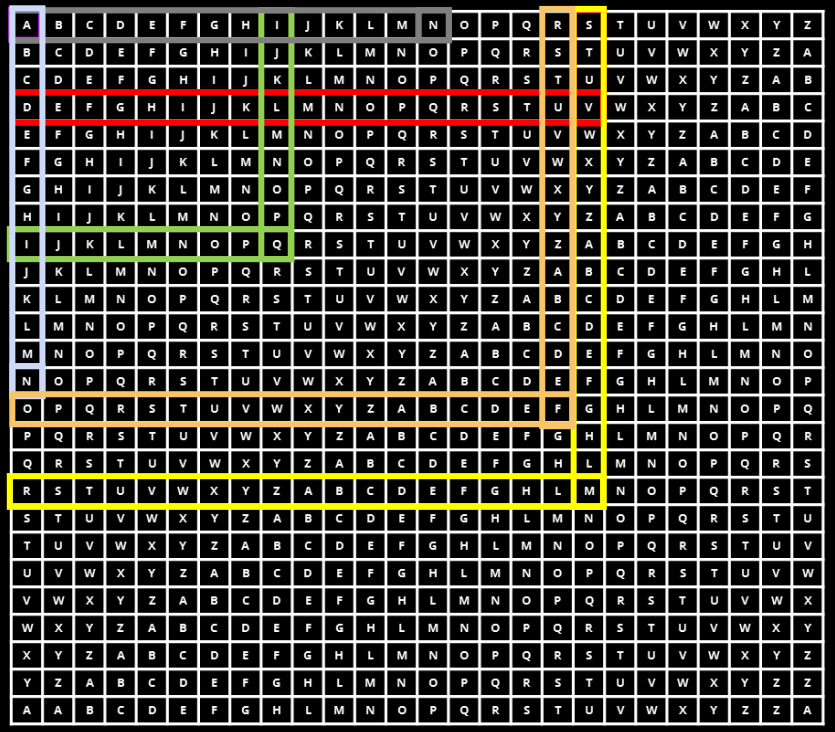
  Texto simples: `Adriano`

  Texto cifrado: `anoAdri`

- Pode ser usada com a técnica de substituição para aumentar a força.



Cifra de Vigenère



Mensagem: a d r i a n o

Chave: a s s i n a r

Cifra: a v m q n n f

OBRIGADO!

Conceitos de Criptografia