

Criptografia de chave simétrica

Segurança da Informação
Curso Técnico em Redes de Computadores
ETER – FAETEC - Rio de Janeiro - RJ

O que é criptologia?

- A criptoanálise é um ramo da matemática que estuda princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, e vice versa.
- Logo, criptografia é o processo de tornar o conteúdo ilegível, e a criptoanálise, o processo inverso, de tornar o conteúdo novamente legível, mas sem ter a chave para desfazer o processo.

Alguns termos.

- Texto em claro, ou texto plano: mensagem original.
- Texto cifrado: mensagem codificada.
- Cifra: algoritmo usado para transformar texto plano em texto cifrado.
- Chave: informação usada na cifra, conhecida apenas por quem envia e/ou recebe a mensagem.
- Código: método de substituição de palavras inteiras, mantendo a estrutura sintática da linguagem original.
- Cifragem (ou encriptação): converter texto plano em texto cifrado.

Mais alguns termos.

- Decifragem (ou deciptação): converter texto cifrado em texto plano.
- Método da força bruta: método usado para quebrar a chave de criptografia tentando exaustivamente todas as combinações possíveis.
- Sistema de chave simétrica: A mesma chave é usada para cifragem e decifragem da mensagem.
- Sistema de chave pública: Uma chave (pública) é usada para cifragem, e outra chave (privada) é usada para decifragem.

Qual é a importância da criptografia?

- A criptografia, numa defesa de perímetro em uma rede de computadores é “a última barreira a ser transposta”: Mesmo se o atacante burlar o firewall, o IDS e outras proteções, se os dados estiverem criptografados, o atacante terá dificuldades para comprometer a confidencialidade daquela informação.

Um pouco de história.

- Criptografia é quase tão antigo quanto as origens da escrita. Seu uso é muito amplo, mas sempre com o objetivo de esconder segredos de leitores pouco bem-vindos.
- Alguns exemplos históricos são a cifra de Cesar (usada no Império Romano), as máquinas Enigma e o Colossus (usados na Segunda Guerra Mundial), entre muitos outros.
- Sugestão: O filme “O Jogo da Imitação” (2014) conta a história da construção do Colossus, usado para quebrar a cifragem nazista.

Classificação das cifras.

1) Tipo de operação usada para transformar o texto em claro em texto cifrado:

- Substituição: Partes do texto em claro são substituídos por texto cifrado.
 - Substituição polialfabética: Diferente para cada caractere.
- Transposição: Partes do texto em claro são rearranjados, usualmente em uma ordem complexa.

Classificação das cifras.

2) Número de chaves usadas:

- Simétrica (uma chave).
- Assimétrica (duas chaves).

3) A forma pela qual o texto em claro é processado:

- Bloco: Um bloco por vez.
- Corrente (ou fluxo): Um elemento por vez.

Uso de números aleatórios na criptografia.

- Há muitos usos:
 - Usos únicos em protocolos de autenticação para evitar repetição.
 - Chaves de sessão.
 - Geração de chaves públicas.
 - Geração de chaves únicas para conexões únicas.
- Estes números devem ser independentes uns dos outros, atenderem uma distribuição uniforme e serem incapazes de preverem os próximos números com base nos números atuais.

Os PRNGs.

- Os Pseudo Random Number Generators (PRNGs), ou Geradores de Números Pseudo Aleatórios, são programas que usam algoritmos determinísticos para criar esses números.
- Na verdade eles não são realmente aleatórios, mas passam em vários testes de aleatoriedade.

A cifra de Cesar (substituição).

- Alfabeto:

abcdefghijklmnopqrstuvwxyz

- Chave usada - deslocamento à direita por 3 caracteres:

defghijklmnopqrstuvwxyzabc

- Texto em claro:

Nos vemos depois da aula

- Texto cifrado:

Qrv yhprv ghsrlv gd dxod

Cifra de substituição polialfabética.

- Aqui, substituímos bits sem alterar as posições, usando alfabetos cifrantes para criptografia.
- No exemplo ao lado, temos a tabela usada pela cifra de Vigenère.
- Uma vantagem dessa cifra é que ela não pode ser quebrada usando análise de frequência.

--PLAINTEXT--

	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

Exemplo da cifra de Vigenère.

- Logo, vamos supor que usaremos como chave a frase **Turma de SI**, e a mensagem é **Nos vemos depois da aula**.
- Realizando a cifragem, teremos a seguinte mensagem cifrada: **GIJ VLPSZ LXJFUS GE SCEU**.
- O texto a ser cifrado é combinado com a chave, que determina qual das diferentes tabelas deve ser usada para cifrar cada letra do texto.

O RC5.

- O Rivest Cypher 5 (RC5) foi criado por Ron Rivest, em 1994, e traz algumas características, como:
 - Cifra de bloco, pode ser implementada em software ou diretamente no hardware.
 - Ela é rápida e simples, adaptável para processadores de diferentes comprimentos de palavra.
 - Trabalha com blocos de tamanho variável (32, 64, 128 bits) e pode trabalhar com um número variável de rodadas (de 0 a 255).
 - Pode operar com chaves de 0 a 2040 bits, requer pouca memória e tem alta segurança.
 - <https://bit.ly/ARCFIVE>

Cifra de transposição colunar

- Texto em claro:

Nos vemos depois da aula

- Chave:

TurmaSI

- Arranjo em quatro linhas e a consequente ordenação:

TURMASI

AIMRSTU

NOS VEM

VM SENO

OS DEPO

EOD POS

IS DA A

AAD IS

ULA

A UL

- Texto cifrado:

VEA MOA DD S AEP NOIUOSSL

A cifra zigue-zague (ou cifra da cerca ferroviária - transposição).

- Texto em claro:

Nos vemos depois da aula

- Arranjo em três linhas:

N	V	S	P			A		
O	E	O	E	O	S	D	U	A
S		M	D	I	A		L	

- Texto cifrado:

Nvsp ao eo eosd uasmdial

Cifra de transposição com a caixa S.

- A caixa S (caixa de substituição), ou matriz S, é um componente básico de cifras simétricas. Matematicamente são funções booleanas vetoriais.
- Abaixo temos uma matriz S usada pelo algoritmo DES, mapeando 6 bits de entrada em 4 bits de saída.

S5		Entrada: Os 4 bits do “meio”															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Os 2 bits das “pontas”	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Exemplo do algoritmo DES.

- Logo, vamos supor que usaremos como chave a frase **Redes**, e a mensagem é **Nos vemos depois da aula.**
- Realizando a cifragem, teremos a seguinte mensagem cifrada:

**fbdpSFZsfTu/669nEh2P4+vC/2JR2YL/
6E5X6c+PnJk=**

- Cada caracter é convertido, segundo a tabela ASCII, para o seu equivalente em binário. Logo, os bits mais externos são usados nas colunas, e os mais internos, nas linhas. A combinação deles é então pega na tabela, e convertida de volta para a tabela ASCII.

Alguns sites para experimentar as cifras.

- Cifra de Cesar: https://bit.ly/cifra_de_cesar
- Cifra de Vigenère: https://bit.ly/cifra_de_vigenere
- Cifra de transposição colunar: https://bit.ly/cifra_colunar
- DES: https://bit.ly/algoritmo_DES
- Cifra de zigue-zague: <https://bit.ly/cifr>

Exemplos de protocolos de criptografia simétrica.

- DES (Data Encryption Standard).
- 3DES (triplo DES).
- AES (Advanced Encryption Standard).
- IDEA (International Data Encryption Algorithm).



Cifras de corrente.

- Essas cifras já foram muito populares, há um tempo atrás.
- Aqui, uma chave é uma entrada para um gerador de bits pseudo-aleatórios, que produz uma aparente sequência de bits aleatórios.
- Esses bits sofrem uma operação lógica (XOR, ou OR exclusivo) com a mensagem para cifrá-la. Para decifrar, basta fazer a mesma operação lógica novamente.

Características das cifras de corrente.

- São eficientes se implementadas diretamente no hardware.
- Longos períodos sem repetição.
- Estatisticamente aleatórios.
- Dependem de uma chave grande o bastante.
- Complexidade linear grande.
- Podem ser tão seguras quanto uma cifra de bloco, só que são mais simples e mais rápidas.

Exemplos de cifras de corrente: A5/1

- A família A5/1 e A5/2 é baseada em registradores de deslocamento (usa três) e é usada no sistema de telefonia GSM para trazer confidencialidade. <https://bit.ly/A5-1>

Exemplos de cifras de corrente: RC4

- O Rivest Cypher 4 (RC4) é um algoritmo patenteado pela RSA Security.
- Ela é baseada em uma permutação aleatória, com chaves de tamanho variável. Mas não se deve reaproveitar chaves.
- É muito usada, em protocolos de segurança para redes sem fio (WEP e WPA), e no protocolo SSL/TLS, para segurança via Web. <https://bit.ly/ARCFOUR>

Tamanho das chaves de criptografia.

- São medidas em bits: 64, 128, 256, 1024 bits, etc.
- Se você deseja dobrar o tamanho das chaves, basta somar mais um bit à chave. Logo, aumentar de uma chave de 128 para 256 bits significa aumentar a complexidade em 2^{128} vezes.
- Logo, se um computador consegue quebrar uma chave de 128 bits em um segundo, ele levaria 2^{128} segundos (algo em torno de $107.902.831 \times 10^{20}$ milênios) para quebrar uma chave de 256 bits.
- Ou seja, é **computacionalmente intratável**. Mas o tamanho da chave não é o único fator a ser levado em conta, mas também o protocolo de criptografia usado junto com a chave.

Criptanálise.

- Uma cifra é **computacionalmente segura** se o texto cifrado atinge um dos seguintes critérios:
 - 1) O custo de quebrar a cifra excede o valor da informação.
 - 2) O tempo requerido para quebrar a cifra excede o tempo de vida útil da informação.
- Logo, uma cifra é **computacionalmente insegura** se algum dos critérios acima não foi atingido.
- O objetivo é a decifragem da mensagem, mas também obter a chave.

Ataques por força bruta.

- Tendo o texto cifrado, este ataque consiste em exaustivamente tentar todas as chaves possíveis.
- É o ataque mais fácil de se defender, visto que o atacante tem pouca informação disponível.
- Alguns chips de custo mais baixo hoje em dia podem fazer essa abordagem de forma mais razoável.
- O maior problema, nesse caso é manter a segurança da chave.

Tempo médio necessário para quebra de chave pelo método da força bruta.

Fundamentos da criptografia.

- Princípio de Kerckhoffs: Enunciado em 1883 por Auguste Kerckhoffs, é a base da criptografia moderna. Ele diz que **a segurança do sistema deve permanecer intacta se tudo sobre ele for revelado, exceto a chave.**

Temporalidade.

- Normalmente, os primeiros pacotes trocados na maior parte das aplicações contêm informações como login e senha. Conhecendo bem os protocolos envolvidos, um atacante pode capturar esses pacotes, mesmo criptografados, e posteriormente iniciar a autenticação com a aplicação e enviar os pacotes com login e senha criptografados quando for solicitado. O atacante poderá ter acesso ao sistema sem ter decifrado a mensagem.
- Ataques de **repetição** usam esse método. A maioria dos sistemas modernos insere dados temporais em cada informação criptografada (como data e hora), fazendo com que a informação seja usada apenas uma vez.

Redundância

- Temos uma aplicação cujos pacotes tem um campo com quatro caracteres numéricos, cifrados pela origem antes do envio. O receptor deve decifrar essa informação, interpretá-la e agir de acordo com ela.
- O atacante pode alterar aleatoriamente os dados desse campo e repassar o pacote. Como o campo não está conforme o esperado, a aplicação descarta a informação ou repassa para camadas superiores.
- O atacante observará o comportamento da aplicação, e com tempo e motivação suficientes, encontrará algum resultado adequado. Este é o ataque de **preenchimento aleatório**.
- A prevenção consiste em usar informações redundantes para verificar a integridade da informação.

A cifra de Feistel

- Horst Feistel criou esta cifra quando trabalhava na IBM, em 1973.
- A **cifra de Feistel** é o método usado para cifragem. A mensagem é dividida em blocos de 64 bits, que são:
 - 1) Permutados segundo duas matrizes (IP e IP¹).
 - 2) Cifra blocos de 32 bits alternadamente em 16 iterações.
 - 3) Permutados novamente, segundo as mesmas matrizes.
- Virtualmente, todas as cifras de bloco mais recentes (como a DES) são baseadas na Cifra de Feistel.

Protocolos de criptografia simétrica: DES.

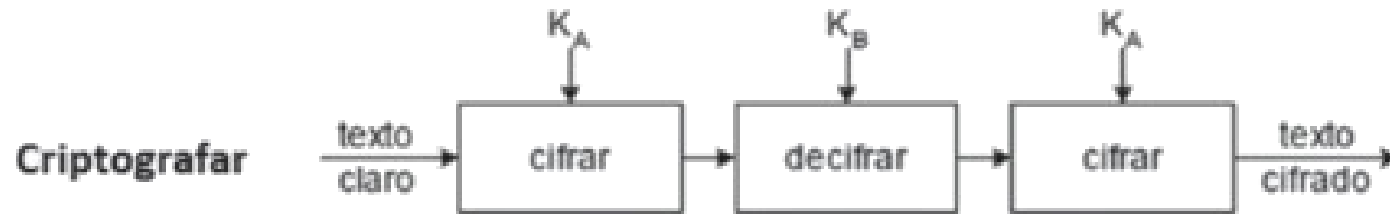
- Data Encryption Standard.
- É baseado em cifras de substituição e transposição.
- É baseada na cifra de Feistel, e foi padronizada em 1977.
- Foi considerado o padrão de criptografia do governo dos EUA, e teve um desenvolvimento controverso:
 - Teve o envolvimento secreto da NSA.
 - O processo de design do algoritmo foi sigiloso.
 - O comprimento da chave foi reduzido de 128 para 56 bits.
- Hoje a sua versão original é considerada insegura, mas afirma-se que uma chave de 128 bits é virtualmente inquebrável por força bruta.

Protocolos de criptografia simétrica: DES.

- O DES é uma variação da Cifra de Feistel.
- O texto em claro é processado em blocos de 64 bits, sendo esses blocos cifrados e temos uma saída do mesmo tamanho.
- Usa chaves de 64 bits, onde 56 bits são a chave e 8 bits são usados para paridade.
- São usadas 16 subchaves em 16 rodadas.
- A segurança é fortemente dependente das “caixas S”.

Protocolos de criptografia simétrica: 3DES.

- Triple Data Encryption Standard.
- Basicamente é a aplicação do DES três vezes seguidas sobre o bloco de 64 bits, e no exemplo abaixo, usando 2 chaves diferentes (K_a e K_b).
- Como são duas chaves de 64 bits, dizemos que o 3DES usa uma chave de 128 bits.
- Usado em aplicações financeiras, e adotado em algumas aplicações na Internet, como PGP e S/MIME. Mas ainda assim é lento e trabalha com blocos pequenos.
- <https://bit.ly/TripleDES>



Protocolos de criptografia simétrica: AES.

- Advanced Encryption Standard.
- Padrão largamente usado em cifragem simétrica e muito usado em aplicações modernas.
- Foi criado pelos belgas Vincent Rijmen e Joan Daemen, padronizado em 1997, após vencer um concurso mundial.
 - Nesse concurso, a NSA se envolveu publicamente!
 - O processo foi todo transparente, e vários algoritmos foram propostos, sendo o AES o vencedor.
- Sua documentação é pública.

Como funciona o AES?

- Ele não usa uma cifra de Feistel, mas cifra blocos de entrada com 128 bits e gera saída cifrada com o mesmo tamanho.
- Pode usar chaves de 128, 192 e 256 bits.
- Usa uma matriz de estado e quatro transformações básicas.
- Dependendo do tamanho da chave, pode ocorrer 10, 12 ou 14 rodadas.
- https://bit.ly/algoritmo_AES

A cifra de Rijndael.

- Esta cifra usa uma matriz quadrada de 4^a ordem, a **matriz de estado**.
- Esta matriz no início do processo com os bits do texto em claro, e no final terá os bits do texto cifrado.
- São quatro transformações que são feitas repetidamente, de 10 a 14 vezes.

Outros protocolos de cifra de bloco: IDEA e Blowfish.

- O IDEA (International Data Encryption Algorithm) foi criado em 1991 por James Massey e Xuejia Lai. Ele trabalha com blocos de 64 bits e chaves de 128 bits. Tem uma implementação por software mais simples do que o DES e é usado no PGP.
- Blowfish: É de implementação simples, é rápido e consome muito pouca memória (menos de 5 Kb!). Ele também trabalha com blocos de 64 bits, e chaves de até 448 bits. Ele foi criado por Bruce Schneier, e é quase uma cifra de Feistel.

Outros protocolos de cifra de bloco: RC6, Twofish, Serpent e CAST-128.

- O RC6 foi criado por Ron Rivest, da RSA Security. Ele trabalha com blocos de tamanho variável, chaves de tamanho variável e número de rodadas variável. Foi um dos finalistas do concurso que elegeu o AES.
- Twofish: Criado por Bruce Schneier. Outro finalista no concurso AES.
- Serpent: Criado por Ross Anderson, Eli Biham e Lars Knudsen. Finalista no concurso AES.
- CAST-128: Foi usado em versões do PGP e do GPG. A chave pode ter de 40 a 128 bits. Foi criado em 1996 por Carlisle Adams e Stafford Tavares.

Resumo.

- Criptografar é escrever informações usando métodos de cifragem; criptoanalisar é tentar descobrir alguma informação que foi criptografada; criptologia é a ciência que envolve criptografia e criptoanálise.
- A segurança da criptografia depende da complexidade do algoritmo e do tamanho da chave utilizada; cada bit a mais na chave tende a dobrar a segurança do sistema.
- Chaves muito grandes para salvar algoritmos ruins podem tornar seu uso inviável.
- A criptografia simétrica cifra e decifra usando a mesma chave, que deverá ser compartilhada a priori entre as partes envolvidas.
- O princípio de Kerckhoffs é a base da criptografia moderna. Ele diz que o algoritmo de criptografia pode e deve ser divulgado; a chave deve ser mantida em segredo.
- Tradicionalmente os algoritmos usavam cifras de substituição e cifras de transposição. A substituição mantém o tamanho do texto original; a transposição pode alterar o tamanho do texto.

Resumo.

- O DES foi o primeiro protocolo de criptografia a se tornar padrão mundial. Ele é simétrico, cifra blocos de 64 bits de texto usando chaves de 56 bits por meio de várias iterações que embaralham a informação usando o algoritmo de Feistel.
- O 3DES é nada mais que o DES aplicado em três etapas (cifra-decifra-cifra, para criptografar, e decifra-cifra-decifra, para decriptografar) e duas chaves diferentes; quando as chaves são iguais, o 3DES e o DES são compatíveis um com o outro.
- O AES é o estado-da-arte em criptografia simétrica; é infinitamente mais seguro que o DES e muito mais seguro que o 3DES.
- O AES é simétrico, cifra blocos de 128 bits de texto usando chaves de 128, 192 ou 256 bits por meio de iterações que embaralham o texto usando o algoritmo de Rijndael.