

Segurança Informática

Aula 2

Docente: Ricardo Costa
rcosta@estg.ipp.pt

Programa

1. Conceitos introdutórios
2. Criptografia básica
3. Autenticação e Controlo de Acessos
4. Ameaças à segurança
5. Penetração em redes e sistemas
6. Políticas de segurança
7. Mecanismos de protecção e técnicas de defesa
8. Entidades de Segurança

2. Criptografia básica

Objetivos:

- * Compreender a importância da criptografia e enunciar sistemas criptográficos.

Princípios de Criptografia

- ▶ Uma das ferramentas mais importantes para a segurança da informação.
- ▶ Qualquer método que transforme informação legível em informação legível/ilegível (Código, cifra).
- ▶ Não resolve todos os problemas de segurança. Não é à prova de falhas.



Princípios fundamentais de Criptografia

▶ Redundância

- ▶ Técnica que visa evitar que um intruso tente enviar dados que possam ser considerados válidos pelo recetor numa transmissão. É inserido propositadamente dados redundantes. Por outro lado, a redundância pode facilitar aos criptoanalistas a descoberta com maior facilidade do conteúdo da informação.

▶ Exemplo:

- ▶ 16 bytes nome cliente (simples), seguido por 3 bytes (1 para quantidade, 2 para o código de produto).
- ▶ Problema: Quase todas as mensagens de 3 bytes recebidas serão consideradas válida
- ▶ Solução: Ampliar parte cifrada para 12 bytes. 9 primeiros bytes com zero.

▶ Atualidade / Evitar reutilização de mensagens

- ▶ Princípio que tenta evitar que indivíduos utilizem a mesma mensagem mais de uma vez. É usado mecanismos de hora para validar uma mensagem.



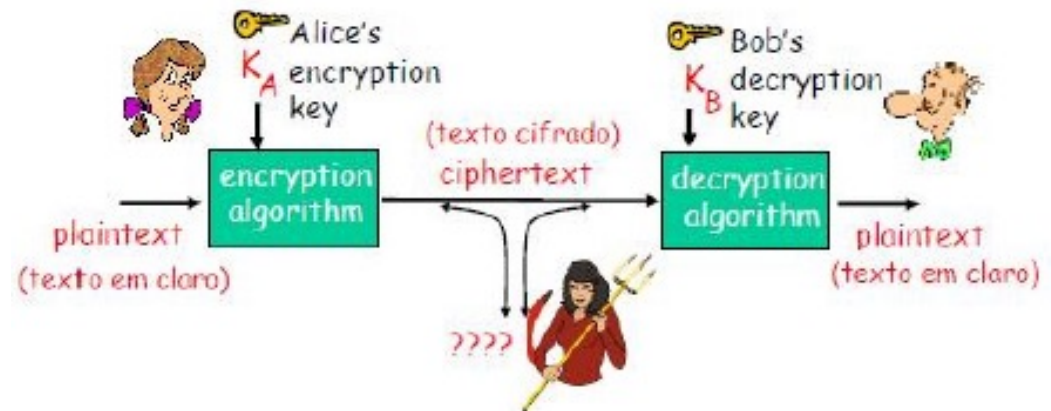
A linguagem da Criptografia

► Chave simétrica

- remetente e destinatário usam chaves idênticas.

► Chaves públicas

- chave de encriptação pública, chave de descriptação secreta (privada).



Conceito de Cifra

- ▶ Transformação de carater por carater, ou bit por bit, sem ter em atenção a estrutura linguística da mensagem.

- ▶ Cifra de Substituição

- ▶ Método que opera de acordo com um sistema pré-definido de substituição.
- ▶ As cifras de substituição são decifradas pela substituição inversa.
- ▶ Existem diversos tipos de cifras de substituição:
 - ❑ **Cifra de substituição simples – Cifra com letras isoladas**
 - ❑ **Cifra de substituição poligráfica – Cifra com grupos de letras**
 - ❑ **Cifra monoalfabética - usa uma só substituição fixa na mensagem inteira**
 - ❑ **Cifra polialfabética - usa mais que uma substituição fixa na mensagem inteira**

- ▶ Cifra de Transposição

- ▶ Método onde as unidades do texto a cifrar são colocadas numa ordem diferente e habitualmente complexa, mas não modificadas. Por contraste, numa cifra de substituição, as unidades do texto são mantidas na mesma ordem, mas elas próprias são alteradas.



Conceito de Código

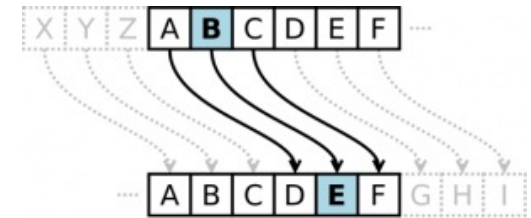
- ▶ Substitui uma palavra por outra palavra ou por um símbolo.
- ▶ A sua utilização é limitada nos tempos atuais.

Criptografia de Chaves Simétricas

- ▶ Cifra de substituição
 - ▶ substitui-se um valor por outro de acordo com uma regra
 - ▶ cifra monoalfabética
 - substitui-se uma letra por outra
- ▶ plaintext: abcdefghijklmnopqrstuvwxyz
- ▶ ciphertext: mnbvcxzasdfghjklpoiuytrewq
- ▶ Exemplo:
 - ▶ Plaintext: bob. i love you. Alice
 - ▶ ciphertext: nkn. s gktc wky. Mgsbc
- ▶ Qual a dificuldade de quebrar esta cifra simples?

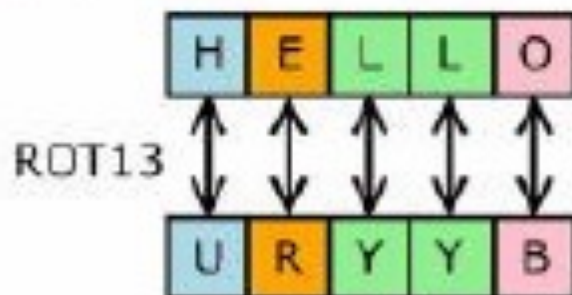
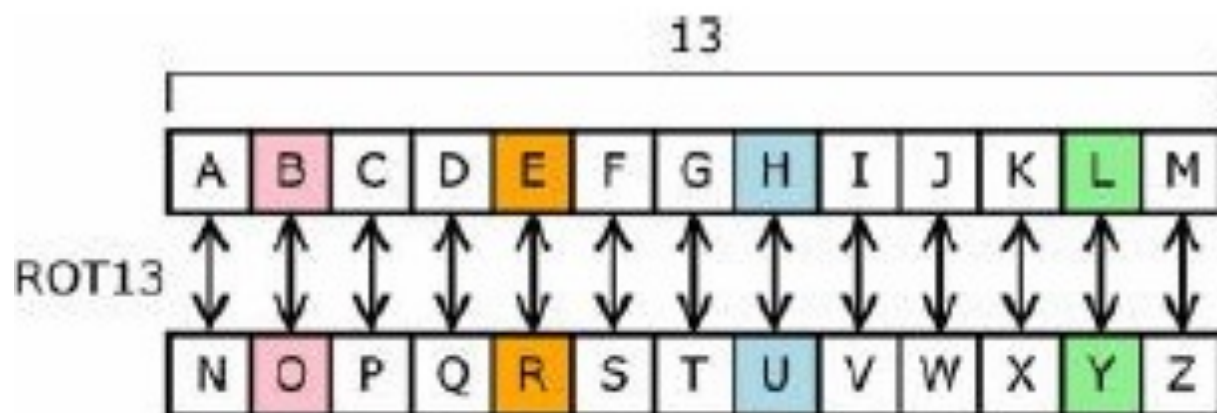
Cifra de César

- ▶ Uma das cifras mais conhecidas e que foi utilizada por Júlio César para este comunicar com as suas tropas durante as guerras que travava.



- ▶ Esta cifra é bastante simples, consiste na substituição de uma letra do alfabeto por seu correspondente três casas adiante, ou seja, a letra A é substituída pela letra D, a letra B pela letra E e assim por diante.
- ▶ Neste caso, o algoritmo da cifra é a troca de uma letra por outra em uma determinada posição. E a chave, neste caso, é o número 3.

Exemplo: ROT13



```
ola bom dia  
byn obz qun  
byn obz qun  
ola bom dia
```

Cifra de Vigenère

- Cifra atribuída equivocadamente a Blaise de Vigenère, foi descrita primeiramente pelo italiano Giovan Battista Bellaso, em 1553, na sua obra *La cifra del. Sig. Giovan Batista Bellaso* e por muito tempo foi considerada como *le chiffre indéchiffrable* (a cifra indecifrável) quando, em meados do século XIX, Charles Babbage e Friedrich Kasiski encontraram um método de resolvê-la.

	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

Processo: A mensagem é cifrada com uma chave alfabética; caso a quantidade de caracteres da chave for menor que o tamanho de caracteres da mensagem, a chave será repetida até ambas terem a mesma quantidade de caracteres. Fazendo uma relação entre as duas (a mensagem e a chave), cada letra da mensagem será cifrada com um alfabeto definido pelo caracter da chave ao qual estará relacionada.

Bastão de Licurgo

- ▶ O Bastão de Licurgo ou scytale (bastão, em grego) era uma técnica de cifragem utilizada pelos soldados espartanos, embora alguns estudiosos sugiram que isto seja apenas um mito.
- ▶ O processo consistia em enrolar uma tira de tecido sobre um bastão de largura definida e sobre esta tira escrevia-se a mensagem. Finda a mensagem, a tira era desenrolada e enviada como um cinto por um mensageiro.
- ▶ No destino a tira devia ser enrolada num bastão de largura igual ao qual a mensagem foi escrita. Sendo o bastão da mesma largura a mensagem era revelava.
- ▶ O algoritmo da cifra, neste caso, é o enrolar da tira no bastão e a chave, a sua largura.



Bastão de Licurgo

- ▶ Uma forma de visualizar a distribuição da mensagem é transpô-la para uma tabela. Para isso, dividimos o tamanho da mensagem pelo número de linhas (o que equivale à sua largura) e obtemos a quantidade de colunas.
- ▶ Exemplo de mensagem:
‘Amanhã há exame surpresa. Estudem.’
- ▶ Desprezando-se os espaços em branco e trocando-se os caracteres especiais, teremos a seguinte mensagem a ser cifrada:
‘amanhahaexamesurpresaestudem’.

Bastão de Licurgo

- ▶ Sendo o tamanho do texto de 28 caracteres e a largura do bastão (chave) 4, e a divisão (que pode não ser inteira), o número de colunas deve ser 7, assim:

(preenchimento) → |a|m|a|n|h|a|h| |a|e|x|a|m|e|s| |u|r|p|r|e|s|a| |e|s|t|u|d|e|m|

- ▶ Se a divisão não for inteira, ficam espaços na tabela que podem ser preenchidos com letras do alfabeto:

(cifragem) ↓ |a|m|a|n|h|a|h| |a|e|x|a|m|e|s| |u|r|p|r|e|s|a| |e|s|t|u|d|e|m|

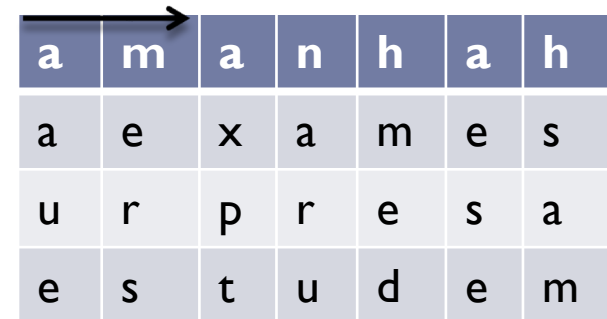
- ▶ O preenchimento da tabela é da esquerda para a direita e de cima para baixo, mas a cifra faz-se de cima para baixo e da esquerda para a direita.

- ▶ Assim, o texto cifrado será: AAUEMERSAXPTNARUHMEDAESEHSAM

Bastão de Licurgo

- ▶ Sendo o tamanho do texto de 28 caracteres e a largura do bastão (chave) 4, o número de colunas deve ser 7.

Se a divisão não for inteira, ficam espaços na tabela que podem ser preenchidos com letras do alfabeto.



a	m	a	n	h	a	h
a	e	x	a	m	e	s
u	r	p	r	e	s	a
e	s	t	u	d	e	m



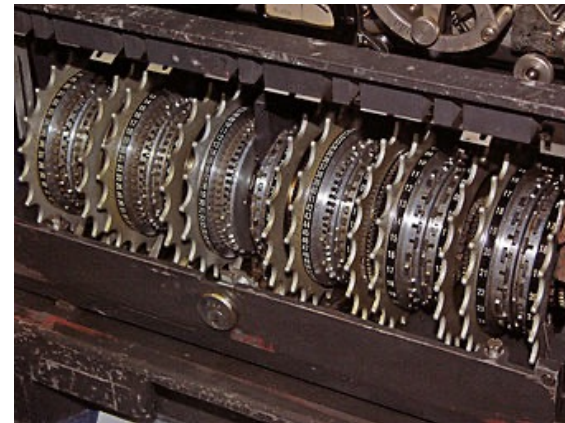
a	m	a	n	h	a	h
a	e	x	a	m	e	s
u	r	p	r	e	s	a
e	s	t	u	d	e	m

O preenchimento da tabela é da esquerda para a direita e de cima para baixo, mas a cifragem faz-se de cima para baixo e da esquerda para a direita.

Assim, o texto cifrado será:
aauemersaxptnaruhmedaesehsam

Lorenz SZ42 cipher machine

- ▶ Máquina alemã, usada pelo Exército durante a Segunda Guerra Mundial.
- ▶ Recurso a cifra de The Vernam



A cifra The Vernam

- ▶ Gilbert Vernam era um engenheiro de pesquisa, na AT&T Bell Labs que, em 1917, inventou um sistema de codificação que usou o sistema Boleano “exclusive or (XOR) função, simbolizada por \oplus .
- ▶ Produz a reciprocidade essencial para permitir que a mesma máquina com as mesmas configurações , possa ser utilizada para cifrar e decifrar.
- ▶ A ideia era usar a prática de telegrafia convencional com uma fita de papel do plaintext combinado com uma fita de papel da chave.

$$\text{Plaintext} \oplus \text{Chave} = \text{texto cifrado}$$

$$\text{Texto cifrado} \oplus \text{Chave} = \text{Plaintext}$$

ENTRADA		SAÍDA
A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Cifra de Transposição

▶ Transposição de colunas

- ▶ A transposição de colunas consiste na escrita de uma chave como cabeçalho da grelha, seguida da mensagem escrita por linhas - sendo a última eventualmente completa por caracteres sem significado.
- ▶ A mensagem é transmitida por colunas, por ordem alfabética das letras no cabeçalho.
- ▶ Por exemplo, se a chave for ZEBRAS, e a mensagem for VAMOS EMBORA, FOMOS DESCOBERTOS, começa-se por obter a grelha:

Z	E	B	R	A	S
V	A	M	O	S	E
M	B	O	R	A	F
O	M	O	S	D	E
S	C	O	B	E	R
T	O	S	J	E	U

Ler-se-ia como:

- ▶ SADEE MOOOS ABMCO ORSBJ EFERU VMOST

(Exemplo retirado da Wikipédia, a enciclopédia livre)



Criptografia de Chaves Simétricas

- ▶ Chave simétrica
 - ▶ Alice e Bob partilham a mesma chave simétrica: K_{AB} .
- ▶ Exemplo: a chave é a regra de substituição na cifra monoalfabética de substituição.
- ▶ Como é que a Alice e o Bob acordam no valor da chave?

Algoritmos de encriptação

- ▶ DES (Data Encryption Standard)
- ▶ AES (Advanced Encryption Standard)
- ▶ TEA (Tiny Encryption Algorithm)
- ▶ RSA (Rivest, Shamir, Adelson)

DES (Data Encryption Standard) - Definição

- ▶ Algoritmo com um pequeno tamanho de chave.
- ▶ O DES foi estudado academicamente e motivou os sistemas modernos de entendimento da criptoanálise.
- ▶ Atualmente é considerado inseguro para muitas aplicações porque:
 - ▶ Tem uma pequena chave;
 - ▶ Em Janeiro de 1999 a distributed.net e a Electronic Frontier Foundation violaram uma chave DES em 22 horas e 15 minutos;
 - ▶ Existem alguns resultados analíticos, obtidos teoricamente, que demonstram a fragilidade da cifra.
- ▶ O DES foi substituído pelo AES.
- ▶ O algoritmo é seguro na forma de 3DES.

3DES - Triple Data Encryption Standard

- ▶ Padrão de criptografia baseado no algoritmo DES, usa 3 chaves de 64 bits.
- ▶ Os dados são encriptados com a primeira chave, desencriptado com a segunda chave e finalmente encriptado novamente com a terceira chave.
- ▶ Isto faz do 3DES ser mais lento que o DES original, mas oferece maior segurança. Em vez de 3 chaves, podem ser utilizadas apenas 2, fazendo-se $K1 = K3$.

DES (Data Encryption Standard) - Descrição

- ▶ O algoritmo recebe uma string de tamanho fixo de um texto plano e transforma, através de uma série de operações, num texto cifrado de mesmo tamanho.
- ▶ O tamanho do bloco é de 64 bits.
- ▶ O DES também usa uma chave para personalizar a transformação, de modo a que a descriptação seja possível por aqueles que conhecem a chave particular utilizada para criptografar.
- ▶ A chave consiste em 64 bits, porém apenas 56 deles são realmente utilizados pelo algoritmo. Os oito bits restantes são utilizados para verificar a paridade e depois são descartados. Assim, o tamanho efetivo da chave é de 56 bits.

-
- ▶ Exemplo de esquema de paridade
 - ▶ As mensagens são partidas em vários blocos de bits.
 - ▶ O número de ocorrências do "1" é contado.
 - ▶ Depois é ativado um bit de paridade : 1 se o número de "1" for ímpar e 0 se o número de "1" for par.
 - ▶ Quando a mensagem chega, é testado o bit de paridade para verificar se está de acordo com o número de "1" da mensagem.
 - ▶ Este esquema tem o problema de falhar quando o número de erros na transmissão é ímpar.
 - ▶ Por exemplo:
 - ▶ K Mensagem enviada: 10010100 - 3 ocorrências de 1 - 3 é ímpar - bit de paridade = 1

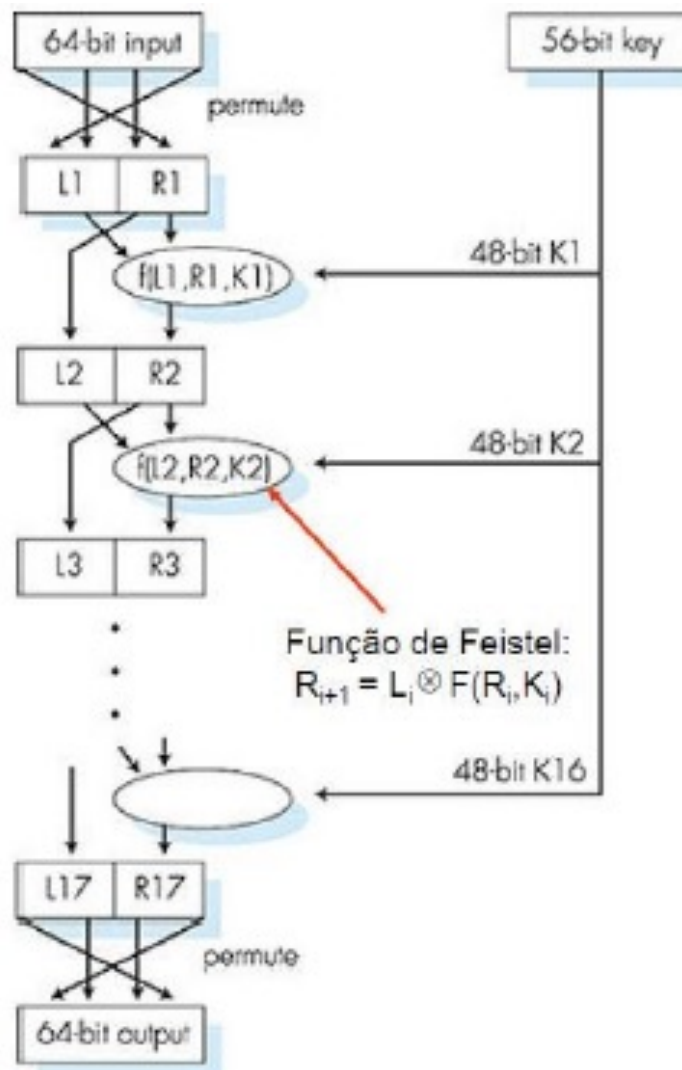
DES (Data Encryption Standard) - Segurança

- ▶ Standard de encriptação US [NIST 1993]
- ▶ Chave de 56-bits, opera em blocos de 64-bits
- ▶ Qual o nível de segurança do DES?
 - ▶ Desafio DES: a frase encriptada com chave de 56 bits (“Strong cryptography makes the world a safer place”) foi descriptada por força bruta em 22 horas em 1999 pelo “EFF Deep Crack”.
- ▶ Não é conhecida uma outra forma de o quebrar
- ▶ Para tornar o DES mais seguro:
 - ▶ Usa-se o 3-DES, que utiliza 3 chaves em sequência em cada bloco de dados.
 - ▶ Utiliza-se blocos de cifra ligados.

DES - Princípio de funcionamento

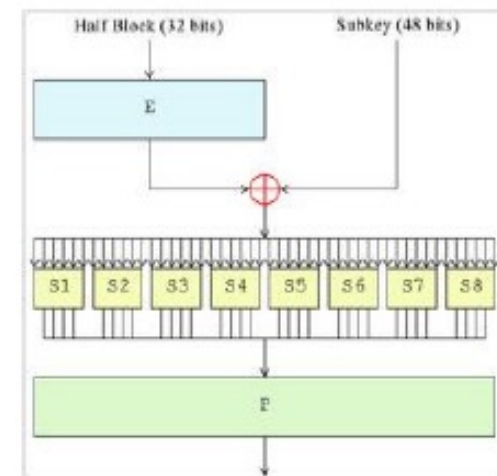
- ▶ Os algoritmos de encriptação do tipo do DES utiliza dois princípios fundamentais para tornar a cifra segura.
- ▶ Difusão:
 - ▶ Cada bit do texto em claro afeta inúmeros bits do texto cifrado.
 - ▶ Torna a relação entre o texto em claro e cifrado difícil de estabelecer.
- ▶ Confusão:
 - ▶ Cada bit da chave afeta inúmeros bits do texto cifrado.
 - ▶ Dificulta a reconstituição estatística do texto em claro a partir de padrões do texto cifrado.

DES - Detalhe do algoritmo



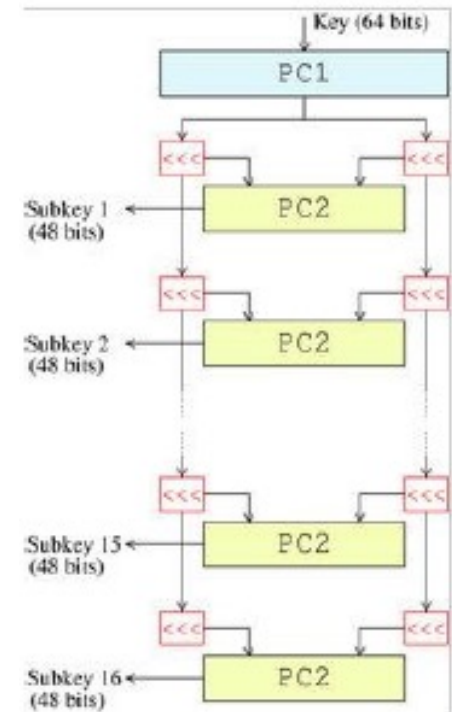
DES - Função de Feistel

- ▶ A função de Feistel, opera em metade do bloco (32 bits) de cada vez e consiste em 4 etapas:
- ▶ Expansão - o bloco de 32 bits é expandido para 48 bits usando a permutação expansiva, representada pelo E , através da duplicação de alguns bits.
- ▶ Mistura de chaves - o resultado é combinado com uma subchave usando uma operação XOR. Dezasseeis subchaves de 48 bits - uma para cada fase – são derivadas da chave principal.
- ▶ Substituição - após trocar a subchave, o bloco é dividido em oito pedaços de 6 bits antes do processamento pelo box de substituição ou S-box. Cada um dos oito S-boxes substitui os seis bits de entrada por quatro bits de saída de acordo com uma transformação não-linear, fornecida por uma lookup table. Os s-boxes fornecem o núcleo da segurança do DES - sem eles, a cifra seria linear e quebrada de forma trivial.
- ▶ Permutação - finalmente, as 32 saídas das S-boxes são rearranjadas de acordo com uma permutação fixa, o P-box.
- ▶ A substituição ocorrida nos S-boxes, a permutação de bits nos P-boxes e a expansão fornecem a chamada "confusão e difusão", respetivamente.



DES - Geração de chaves intermédias

- ▶ Algoritmo que gera as subchaves.
- ▶ Inicialmente, 56 bits da chave são seleccionados dos 64 iniciais para a "Troca escolhida 1" (PC-1).
- ▶ Os oito bits restantes são, ou descartados, ou utilizados como bits de paridade.
- ▶ Os 56 bits são então divididos em dois blocos de 28 bits; cada metade é tratada separadamente. Em fases sucessivas, as duas metades são "rodadas" à esquerda por um ou dois bits (especificado para cada fase) e então uma subchave de 48 bits é seleccionada para a Troca escolhida 2 (PC-2) - 24 bits da metade esquerda e 24 da metade direita.
- ▶ As rotações (representadas como "<<<") significam que um conjunto diferente de bits foi usado em cada subchave; cada bit é usado em aproximadamente 14 das 16 subchaves.
- ▶ Para descriptar é similar - as subchaves estão em ordem inversa, se comparadas com a encriptação. Excepto por essa diferença, todo o processo é o mesmo da encriptação.



DES - Ataques possíveis

- ▶ Brute Force Attack : utilizar todas as combinações possíveis da chave; correr o algoritmo de descriptação e analisar o resultado.
 - ▶ Trabalhoso mas eficaz com clusters (conjunto de computadores, que utilizam sistemas distribuídos) e hardware paralelo.
- ▶ Known Plain Text Attack : conhecendo um texto em claro e a sua versão encriptada, a chave pode ser mais facilmente deduzida.
- ▶ Dictionary Attacks : o atacante consegue estabelecer um conjunto de termos e os seus respetivos valores encriptados.
- ▶ Ciphertext-only attack : a partir do texto encriptado, o atacante consegue estabelecer uma equivalência com texto em claro.
 - ▶ Ex: Análise estatística de termos frequentes.

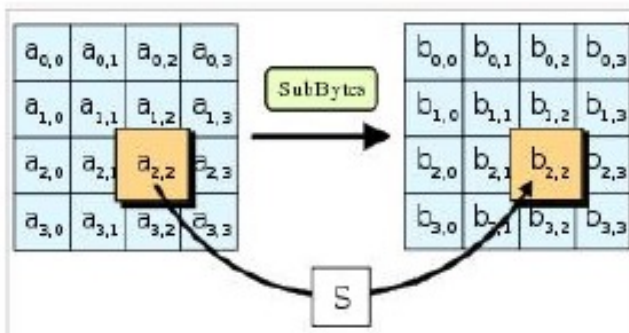
AES (Advanced Encryption Standard) - Definição

- ▶ Também conhecido por Rijndael por causa dos seus criadores Vincent Rijmen e Joan Daemen.
- ▶ Novo (Nov. 2001) standard de chave simétrica do National Institute of Standards and Technology , para substituir o DES.
- ▶ Processa os dados em blocos de 128 bits.
- ▶ Chaves de 128, 192, ou 256 bits.
- ▶ Ataque por força bruta que demora 1 segundo no DES, demora 149 triliões de anos no AES.

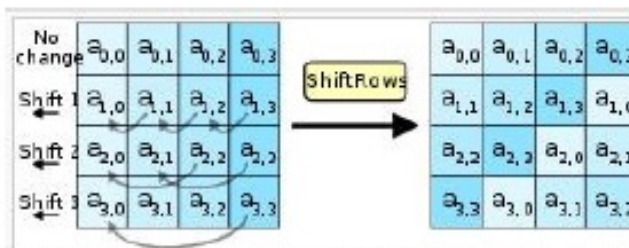
AES (Advanced Encryption Standard) - Fases

- ▶ O AES opera em matrizes de 4x4 bytes, denominados estados.
- ▶ É composto por 4 fases que operam em cada byte do estado:
 - ▶ 1. SubBytes: substituição não linear dos bytes utilizando uma Sbox de Rijndael.
 - ▶ 2. ShiftRows: cada linha do estado é transposta.
 - ▶ 3. MixColumns: os bytes de cada coluna são combinados entre eles .
 - ▶ 4. AddRoundKey: cada byte é combinado com um byte de uma chave de turno.

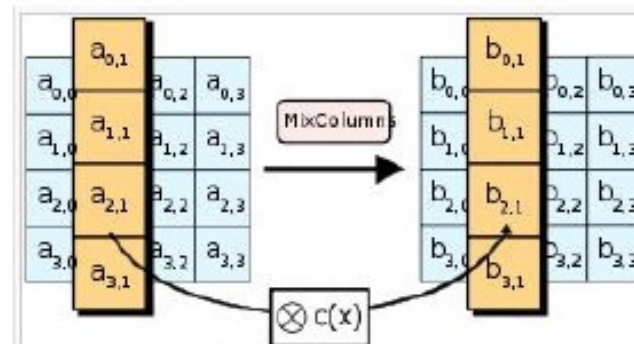
AES (Advanced Encryption Standard) - Fases



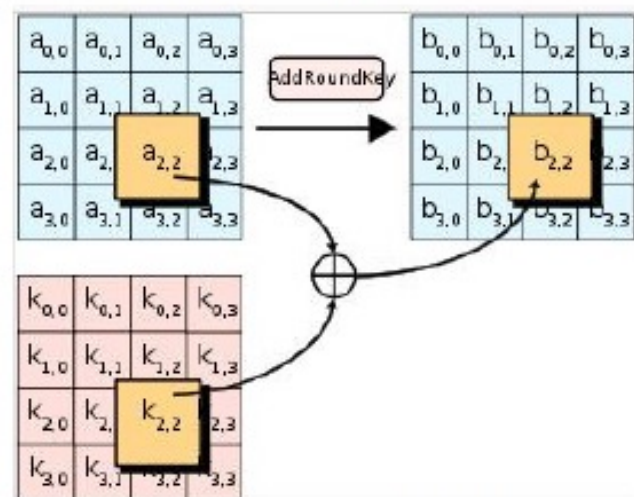
In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S ; $b_{ij} = S(a_{ij})$.



In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.



In the MixColumns step, each column of the state is multiplied with a fixed polynomial $c(x)$.



In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation (\oplus).

TEA (Tiny Encryption Algorithm) - Definição

- ▶ Simples, eficaz e seguro
- ▶ Opera em blocos de 64 bits que divide em dois blocos de 32 bits.
- ▶ Utiliza uma chave de 128 bits que divide em 4 subchaves de 32 bits usada em cada um dos 4 sub-ciclos.

TEA - Criptografia de Chave pública

▶ Chave simétrica:

- ▶ Necessita que o remetente e o destinatário partilhem uma chave secreta.
- ▶ Como combinar qual a chave a utilizar se os intervenientes nunca se encontrarem ?
 - ▶ Problema complexo de resolver !

▶ Chave pública:

- ▶ Remetente e o destinatário não partilham uma chave secreta.
- ▶ Chave de encriptação pública é conhecida pelo remetente (e por todos) .
- ▶ Chave de (des)encriptação privada só é conhecida pelo destinatário.

TEA - Implementações

- ▶ Implementação em JavaScript do TEA.
 - ▶ <http://www.movable-type.co.uk/scripts/tea.html>
- ▶ Implementação em PHP do TEA.
 - ▶ http://www.php-einfach.de/sonstiges_generator_xtea.php

RSA (Rivest, Shamir, Adelson) - Funcionamento

- ▶ São gerados dois pares de números – as chaves – de tal forma que uma mensagem encriptada com o primeiro possa ser apenas desencriptada com o segundo par.
- ▶ O segundo número não pode ser derivado do primeiro. Esta propriedade assegura que o primeiro número possa ser divulgado a alguém que pretenda enviar uma mensagem encriptada ao detentor do segundo número, já que apenas essa pessoa pode desencriptar a mensagem.
- ▶ O primeiro par é designado como chave pública, e o segundo como chave secreta.
- ▶ Embora seja fácil encontrar dois números primos de grandes dimensões, conseguir fatorizar o produto dos dois números é considerado computacionalmente complexo.

RSA (Rivest, Shamir, Adelson) - Funcionamento

- ▶ Todas as mensagens cifradas com chave pública só podem ser decifradas usando a respetiva chave privada. A criptografia RSA atua diretamente na internet, por exemplo, em mensagens de emails, em compras.

1. Escolhem-se dois números primos muito grandes p, q .
(e.g., tais que $p.q$ tenha pelo menos 1024 bits)
2. Calculam-se $n = p.q$ e $z = (p-1).(q-1)$
3. Escolhe-se e ($e < z$) que não tenha factores comuns com z . (e, z são "primos relativamente um ao outro").
4. Escolhe-se $d < z$, tal que $e \times d - 1$ seja exactamente divisível por z , ou seja: $e \times d \bmod (z) = 1$.
5. Chave Publica = (n, e) . Chave Privada = (n, d) .
 $\underbrace{\hspace{1cm}}_{K_B^+} \hspace{1cm} \underbrace{\hspace{1cm}}_{K_B^-}$

RSA - Encriptação e Desencriptação

1. Dadas $K^+ = (n, e)$ e $K^- = (n, d)$ definidas anteriormente
2. Para encriptar uma sequência de bits, m , calcula-se $c = m^e \bmod n$ (i.e. resto da divisão de m^e por n)
3. Para desencriptar a sequência de bits, c , calcula-se $m = c^d \bmod n$ (i.e. resto da divisão de c^d por n)

Ou seja:

$$m = \underbrace{(m^e \bmod n)}_c^d \bmod n$$

RSA (Rivest, Shamir, Adelson) - Exemplo

Bob chooses $p=5$, $q=7$. Then $n=35$, $z=24$.

$e=5$ (so e , z relatively prime).

$d=29$ (so $ed-1$ exactly divisible by z).

encrypt:	<u>letter</u>	<u>m</u>	<u>m^e</u>	<u>c = m^e mod n</u>
	I	12	248832	17
decrypt:	<u>c</u>	<u>c^d</u>	<u>m = c^d mod n</u>	<u>letter</u>
	17	481968572106750915091411825223071697	12	I

RSA (Rivest, Shamir, Adelson) - Exemplo

Alice's RSA encryption, $e = 5$, $n = 35$

Plaintext Letter	m : numeric representation	m^e	ciphertext $c = m^e \bmod n$
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

Bob's RSA decryption, $d = 29$, $n = 35$

Ciphertext c	c^d	$m = c^d \bmod n$	Plaintext Letter
17	481968572106750915091411825223071697	12	l
15	12783403948858939111232757568359375	15	o
22	851643319086537701956194499721106030592	22	v
10	10000000000000000000000000000000	5	e

Comparação de desempenho

	<i>Key size/hash size (bits)</i>	<i>Extrapolated speed (kbytes/sec.)</i>	<i>PRB optimized (kbytes/s)</i>
DES	56	350	7746
Triple-DES	112	120	2842
TEA	128	700	-
RSA	512	7	-
RSA	2048	1	-

Questão de aula

Como interligamos os sistemas informáticos e as mensagens/pacotes com criptografia?

QUESTÕES ?

Docente: Ricardo Costa

rcosta@estg.ipp.pt

