Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Técnicas de Defesa
(Antivírus, Filtro AntiSpam e Criptografia)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

Não existe nenhuma rede 100% segura, mas podemos empregar diversos mecanismos para minimizar problemas relacionados à segurança.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

Os principais mecanismos de segurança a serem utilizados em uma rede de computadores são:

- Antivírus;
- Filtro Antispam;
- Criptografia;
- Firewall;
- Rede Virtual Privada (VPN);
- Autenticação;
- Sistema de Detecção de Intruso;
- Política de Segurança.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução

Em uma rede que empregue corretamente esses mecanismos, os incidentes de segurança serão certamente minimizados, e quando ocorrerem, poderão ser detectados e tratados de forma satisfatória.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta?

O que é Antivírus?

Antivírus

É um *software* que detecta, impede e atua na remoção de programas de *software* maliciosos. Ele varre arquivos ou monitora ações pré-definidas em busca de indícios de atividades maliciosas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus

Em geral, os antivírus operam das seguintes formas:

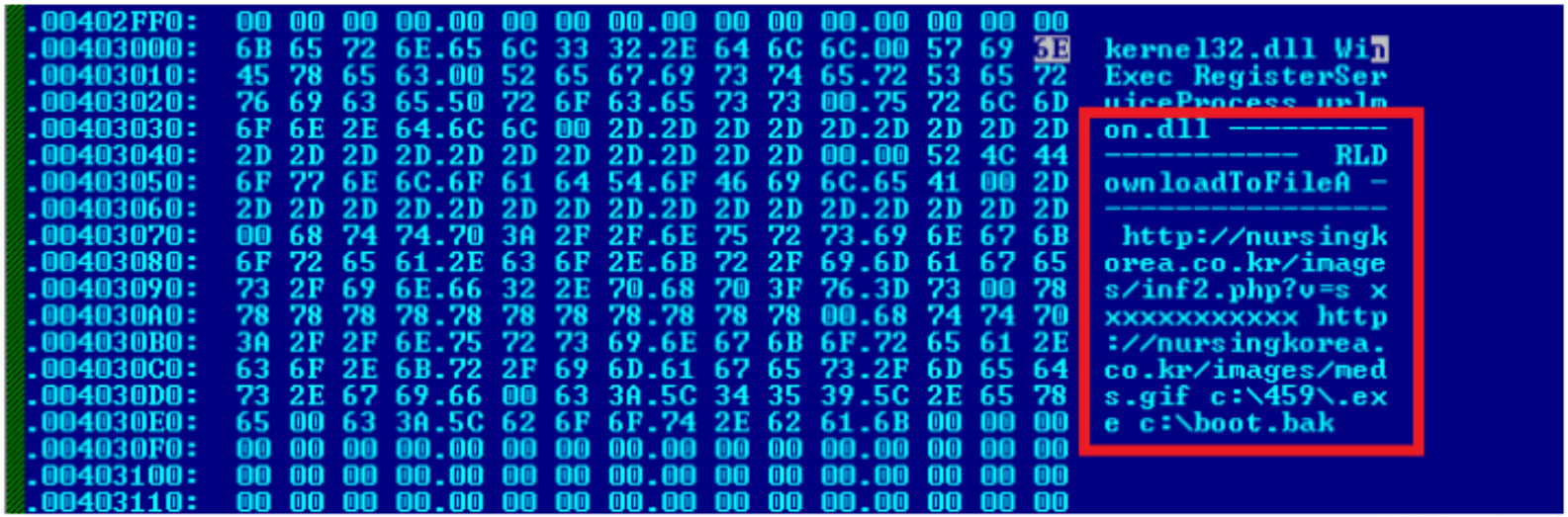
- Assinatura: um arquivo executável é dividido em pequenas porções (*chunks*) de código, as quais são comparadas com a base de assinaturas do antivírus.
- Heurística: um arquivo sob análise é executado virtualmente em um emulador minimalista e os indícios de comportamento suspeito são avaliados a fim de se verificar a atividade realizada pelo programa.
- Comportamental: é feito uma análise do comportamento dos programas que são executados e identificando se determinadas ações são suspeitas (por exemplo, gravação em arquivo executável).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus

Assinatura

Pode ser: um *hashes* criptográficos que identificam o arquivo de forma única, a identificação das funções importadas e exportadas e a obtenção de determinadas cadeias de caracteres, como URLs e endereços de correio eletrônico. Essa assinatura está contida dentro do *malware* ou dos arquivos infectados.



FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus

O grande problema dos antivírus é o surgimento frequente e crescente de variantes de *malware*, cujas ações modificadas visam evadir a detecção.

Muitos exemplares de *malware* possuem mecanismos próprios de defesa cujas ações variam entre desabilitar as proteções existentes no sistema operacional alvo (por exxemplo, *firewall*, antivírus e *plugins* de segurança), verificar se o exemplar está sob análise e disfarçar-se de programas do sistema.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Antivírus

Forma de obtenção

Podem ser gratuitos, experimentais (*trial*, usados livremente por um prazo predeterminado) e pagos. Um mesmo fabricante pode disponibilizar mais de um tipo de programa, sendo que a versão gratuita costuma possuir funcionalidades básicas ao passo que a versão paga possui funcionalidades extras, além de poder contar com suporte.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus

Tipos

- Desktop: é instalado em cada computador existente em sua rede e precisa ser atualizado individualmente em cada um destes computadores.
- Servidor: instalar um programa antivírus (servidor) em um servidor de rede e uma outra versão de antivírus (cliente) nas estações da sua rede. O administrador da rede atualizava a base de dados de vírus somente no servidor. Logo em seguida, o administrador ou o próprio programa antivírus insere uma rotina para que esta atualização seja repassada a todas as estações da rede automaticamente.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus

Dicas

- Tenha sempre um antivírus instalado em seu computador;
- Configure para verificar automaticamente arquivos anexados aos e-mails e obtidos pela Internet, os discos rígidos e as unidades removíveis (como pen-drives, CDs, DVDs e discos externos);
- Mantenha o antivírus e a base de assinatura sempre atualizadas;
- Nunca use dois antivírus no mesmo computador podendo causar instabilidade e não detectar vírus;
- Utilize antivírus *online* quando suspeitar que o seu antivírus esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião sobre um arquivo. O site `https://www.virustotal.com/` disponibiliza um antivírus online.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus

Principais antivírus do mercado

- Kaspersky;
- Bitdefender;
- Avira;
- Avast;
- McAfee;
- AVG.

O site `http://www.av-comparatives.org/` realiza comparações, através de testes, entre diversos antivírus.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta?

O que é filtro Antispam?

Filtro Antispam

- Spam é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.
- Atualmente, os spams estão diretamente associados a ataques a segurança da Internet e do usuário, sendo um dos grandes responsáveis pela propagação de códigos maliciosos, disseminação de golpes e venda ilegal de produtos.
- Os filtros antispam é um *software* já vem integrado a maioria dos Webmails e programas leitores de e-mails e permite separar os e-mails desejados dos indesejados (spams). A maioria dos filtros passa por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas spam e, com base nas classificações, o filtro vai "aprendendo" a distinguir as mensagens.

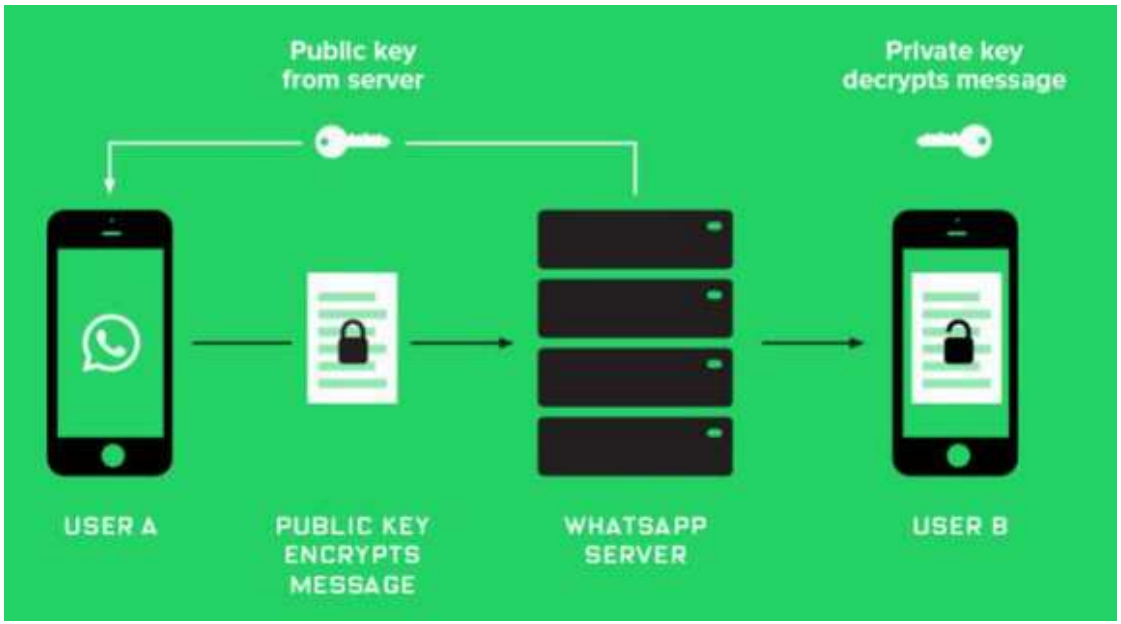
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta?

O que é Criptografia?

Criptografia

É a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica. Esse técnica visa garantir o sigilo e/ou a autenticidade da informação.



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Criptoanálise

Ciência de quebrar códigos e decifrar mensagens; ataque é uma tentativa de criptoanálise.

Criptologia

Ciência que reúne criptografia e criptoanálise.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia

Criptografia é a base para muitas aplicações de segurança:

- Autenticação segura, comunicação segura;
- Dinheiro eletrônico, certificados digitais;
- Identidade digital, assinatura digital.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia

Componentes

A mensagem original, antes de ser transformada, é chamada texto claro. Após transformada, ela é denominada simplesmente texto cifrado. Um algoritmo de criptografia transforma o texto claro em texto cifrado; um algoritmo de decriptografia transforma o texto cifrado de volta para texto claro. O emissor usa um algoritmo de criptografia e o receptor utiliza um algoritmo de decriptografia.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia

Atualmente, os algoritmos criptográficos são divulgados à comunidade e o sigilo das informações é garantido apenas pela chave. Quanto maior a chave, mais dificuldade para um ataque por força bruta.

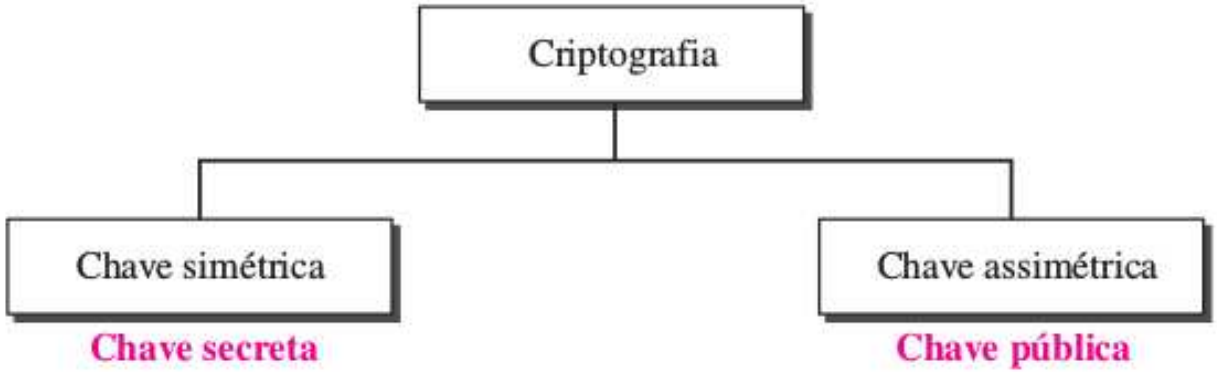
A quebra da criptografia utilizando força bruta (todas as chaves possíveis) é inviável para chaves acima de 128 *bits*, por exemplo:

- Chaves de 64 *bits*: utilizando o computador gerando 90 bilhões de chaves por segundo (*Deep Crack*) temos o tempo de 4 dias e meio para encontrar uma chave.
- Chave de 128 *bits*: utilizando um computador bem melhor (gerando 1 trilhão de chaves por segundo) temos o o tempo de 10 milhões de trilhões de anos para testarmos todas as chaves.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia

Podemos dividir todos os algoritmos de criptografia (cifras) em dois grupos: algoritmos de criptografia de chave simétrica (também chamados chave secreta) e algoritmos de criptografia assimétrica (também denominados chave-pública).



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia

Criptografia de Chave Simétrica

A mesma chave é utilizada por ambas as partes. O emissor usa essa chave e um algoritmo de criptografia para criptografar os dados; o receptor usa a mesma chave e o algoritmo de decriptografia correspondente para decriptografar os dados. A chave precisa ser pré-combinada entre os participantes.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Simétrica

Vantagens:

- Velocidade e algoritmos rápidos;
- Facilidade de implementação em hardware;
- Chaves pequenas e simples geram cifradores robustos.

Desvantagens:

- Distribuição das chaves dificulta gerenciamento. Soluções:
  - Algoritmo Diffie-Hellman para troca de chaves.
  - Utilização de criptografia assimétrica.
- Não permite autenticação e não repúdio do remetente.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Simétrica

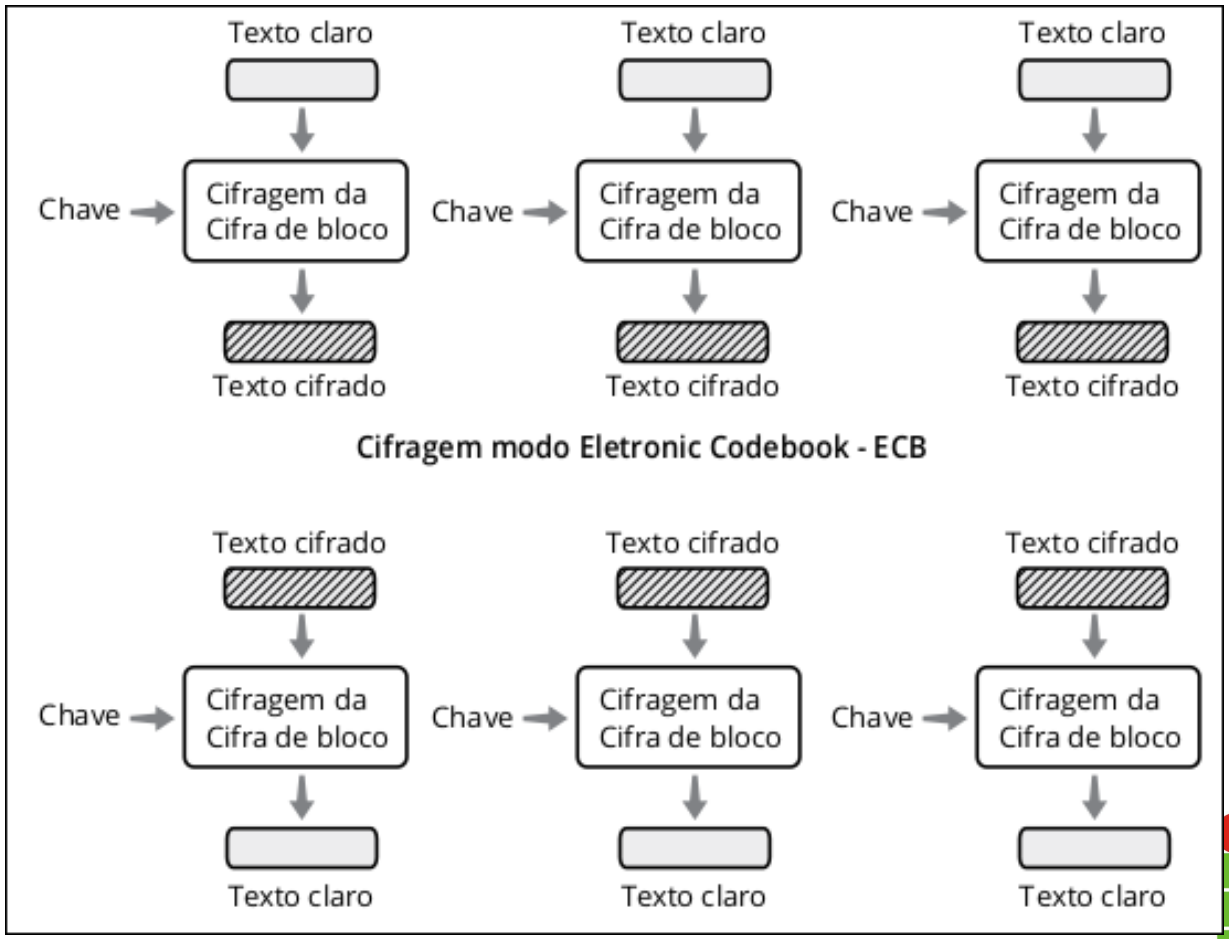
Métodos de crifragem:

- Cifragem por fluxo (streamcipher) é aquela que encripta um fluxo de dados digital um bit ou um byte por vez. Ela é pouco utilizado, fora do escopo da disciplina.
- Cifragem em blocos (block cipher): é aquela em que um bloco de texto claro é tratado como um todo e usado para produzir um de texto cifrado com o mesmo tamanho. Normalmente, um tamanho de bloco de 64 ou 128 bits é utilizado. Elas são subdivididas em:
  - Eletronic Code Book (ECB);
  - Cipher Block Chaining (CBC);
  - Cipher Feed Back (CFB).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Eletronic Code Book:

Método mais simples, cifra bloco de modo independente usando a mesma chave. A mensagem cifrada é obtida por concatenação dos blocos cifrados.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Simétrica

Eletronic Code Book:

Cifra cada bloco de 64 bits de forma independente, usando a mesma chave. O mecanismo ECB não é considerado muito seguro, pois um intruso pode perceber quando uma mensagem muda pela mudança no bloco. No ECB, uma mesma mensagem cifrada várias vezes vai gerar sempre o mesmo bloco.

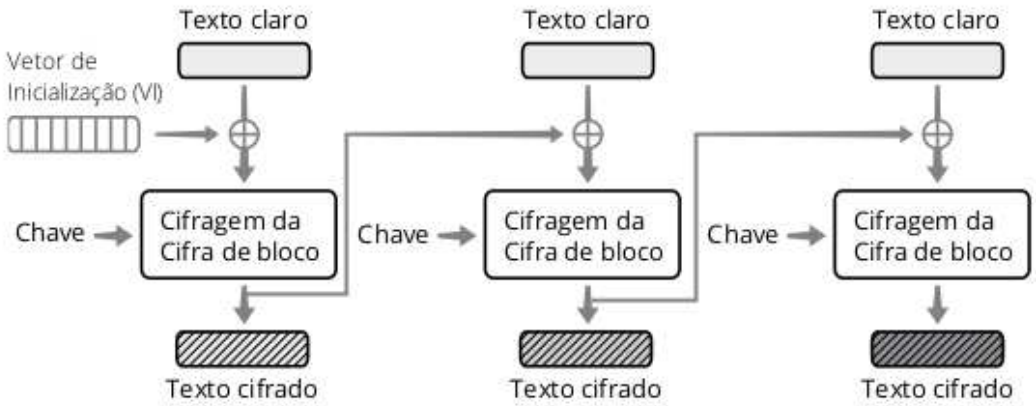
Desvantagens:

- Blocos iguais de textos claros produzem blocos cifrados iguais;
- Não esconde padrão de dados;
- Nada acrescenta à confidencialidade proporcionada pela cifra.

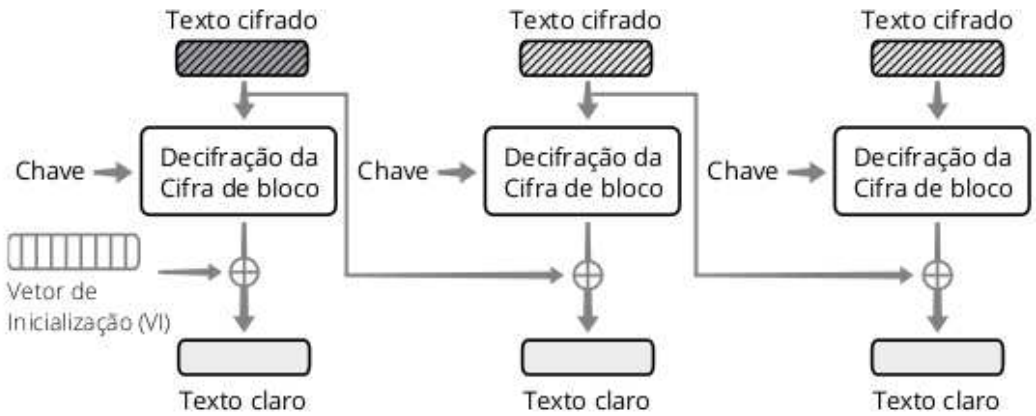
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Cipher Block Chaining:

Nesse modo, cada bloco depende do resultado do bloco anterior. Através de um método chamado feedback, o bloco anterior é utilizado no processo de cifragem do bloco seguinte (Operação XOR).



Cifragem modo Cipher-block Chaining - CBC



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Simétrica

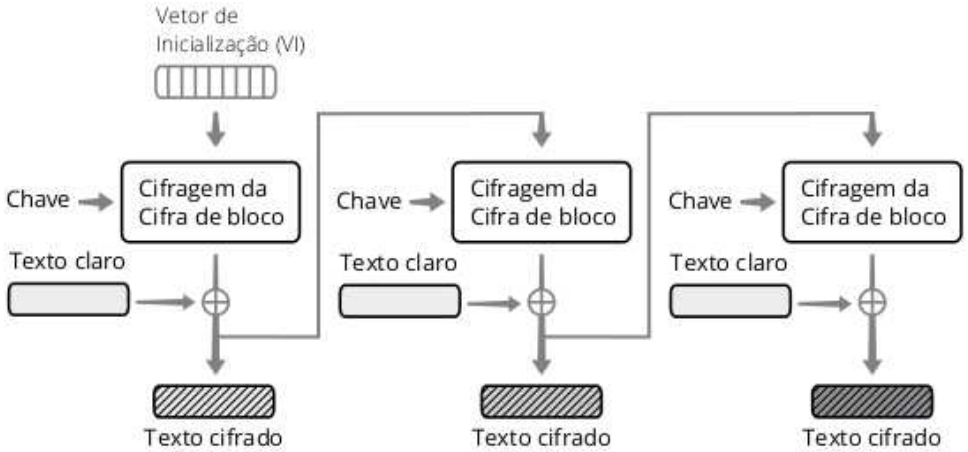
Cipher Block Chaining:

É o modo de operação mais usado. Sua desvantagem é ser sequencial, que não pode ser usado em paralelo e tem maior tempo de processamento. Além disso, um sistema que usa CBC deve garantir que todos os blocos cheguem corretamente, pois um erro em um bloco se propagará para todos os outros.

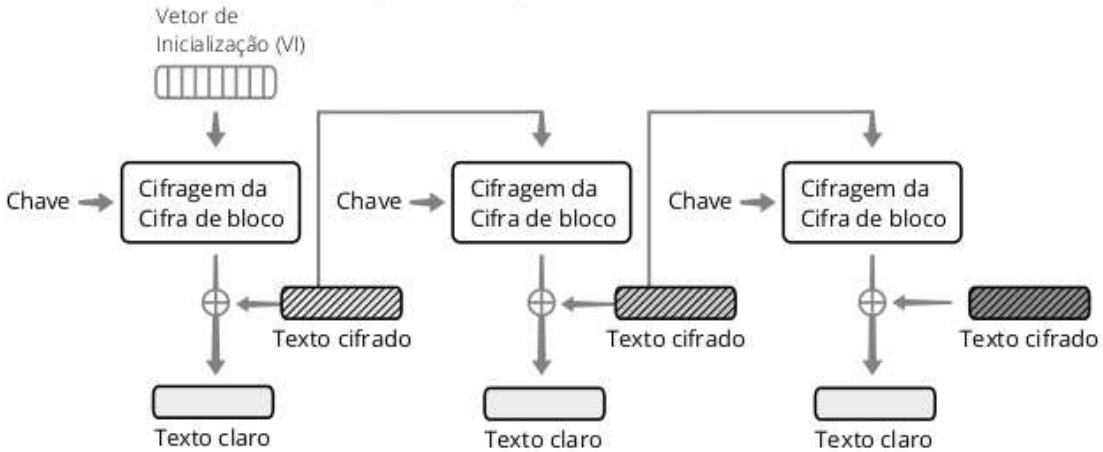
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Cipher Feed Back:

O CFB é capaz de cifrar dados de qualquer tamanho, independentemente do bloco. É útil para cifrar pequenas quantidades de informação ou informações que devem ser imediatamente transmitidas.



Cifragem modo Cipher Feedback - CFB



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Simétrica

Principais algoritmos são:

- DES (inseguro);
- 3DES;
- RC-4;
- AES.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Data Encryption Standard - DES

O Data Encryption Standard (DES) foi padronizado em 1978 pelo ANSI (American National Standard Institute) sob o nome de ANSI X3.92, também conhecido como DEA (Data Encryption Algorithm).

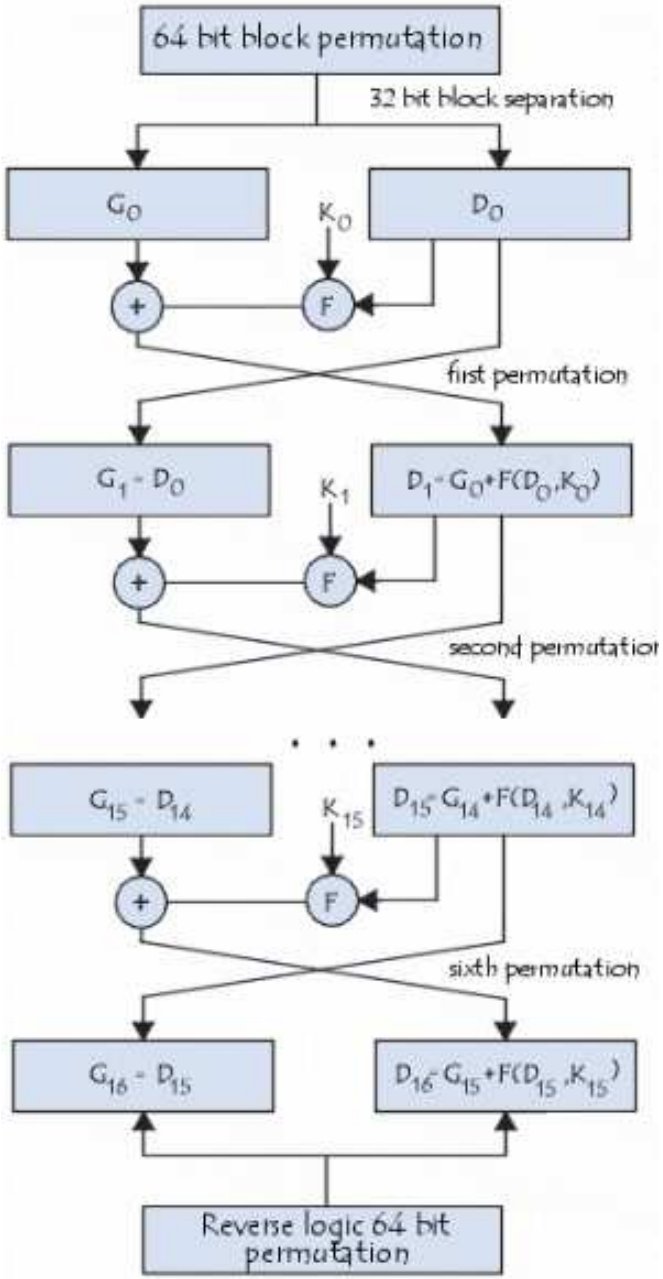
O algoritmo efetua combinações, substituições e permutações entre o texto a ser codificado e a chave. É um sistema de codificação simétrico por chave de 64 bits, dos quais 8 bits (um byte) servem de teste de paridade (para verificar a integridade da chave). Assim, a chave possui um comprimento útil de 56 bits.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Data Encryption Standard - DES

O algoritmo são o fracionamento do texto em blocos de 64 bits (8 bytes), a permuta inicial dos blocos, a partição dos blocos em duas partes: esquerda e direita, chamadas G e D, respectivamente; as fases de permuta e substituição repetidas 16 vezes.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Data Encryption Standard - DES

Permutação inicial

Esta matriz de permutação indica, percorrendo a matriz da esquerda para a direita e, em seguida, de cima para baixo, que o 58º bit do bloco de texto de 64 bits reaparece em primeira posição, o 50º em segunda, e assim, sucessivamente.

PI								
	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8
	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Data Encryption Standard - DES

Cisão em blocos de 32 bits

Depois de realizar a permuta inicial, o bloco de 64 bits é dividido em dois blocos de 32 bits, respectivamente G e D

G_0

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8

D_0

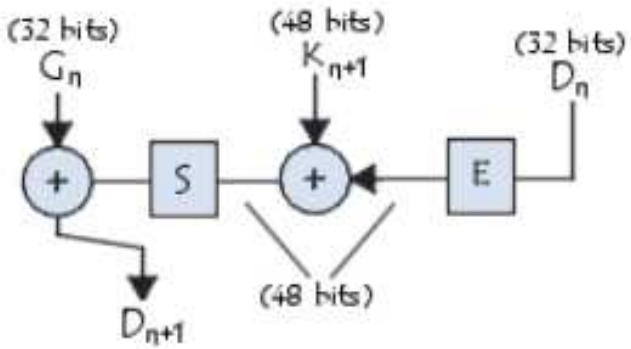
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Data Encryption Standard - DES

Voltas

Os blocos G_n e D_n são sujeitos a um conjunto de transformações iterativas chamadas voltas. Em cada volta tem uma operação de expansão, OU exclusivo com a chave e função de substituição.



Função de expansão

Os 32 bits do bloco D_0 são estendidos a 48 bits através da tabela de expansão, onde os 48 bits são misturados e apenas 16 serão duplicados. Assim, o último bit (32) de D_0 torna-se o primeiro, o primeiro torna-se o segundo, etc. Além disso, os bits 1,4,5,8,9,12,13,16,17,20,21,24,25,28 e 29 de D_0 são duplicados e disseminados na matriz.

E						
	32	1	2	3	4	5
	4	5	6	7	8	9
	8	9	10	11	12	13
	12	13	14	15	16	17
	16	17	18	19	20	21
	20	21	22	23	24	25
	24	25	26	27	28	29
	28	29	30	31	32	1

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Data Encryption Standard - DES

OU exclusivo com a chave

A matriz resultante de 48 bits passa porum OU exclusivo com a primeira chave K_1. O resultado deste OU exclusivo é uma outra matriz de 48 bits.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Data Encryption Standard - DES

Função de substituição

Em seguida, a matriz é dividida em 8 blocos de 6 bits, notado $D0_i$. Cada um destes blocos passa por funções de seleção (chamada também de caixas de substituição), marcadas geralmente como S_i.

Os primeiros e últimos bits de cada $D0_i$ determina (em binário) a linha da função de seleção, os outros bits (respectivamente 2, 3, 4 e 5) determinam a coluna. A seleção da linha, fazendo-se sobre duas bits, tem 4 possibilidades (0,1,2,3). A seleção da coluna sendo feita em 4 bits, tem 16 possibilidades (de 0 a 15). Graças a esta informação, a função de seleção "seleciona" um valor codificado em 4 bits.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Data Encryption Standard - DES

S_1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Suponhamos que $D0_1$ é igual a 101110. Os primeiros e últimos bits dão 10, ou seja, 2 em binário. Os bits 2, 3, 4 e 5 dão 0111, seja 7 em binário. O resultado da função de seleção é, então, o valor situado na linha n° 2, na coluna n° 7. Trata-se do valor 11, ou 111 em binário.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Data Encryption Standard - DES

Por último, o bloco de 32 bits obtido é submetido a uma permuta P cuja tabela é a seguinte.

P								
	16	7	20	21	29	12	28	17
	1	15	23	26	5	18	31	10
	2	8	24	14	32	27	3	9
	19	13	30	6	22	11	4	25

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Data Encryption Standard - DES

OU exclusivo

O conjunto destes resultados em saída de P é submetido a um OU exclusivo com o G_0 inicial (como indicado no primeiro esquema) para dar D_1, enquanto o D_0 inicial dá G_1.

Iteração

O conjunto das etapas precedentes (voltas) é reiterado 16 vezes.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Data Encryption Standard - DES

Permuta inicial inversa

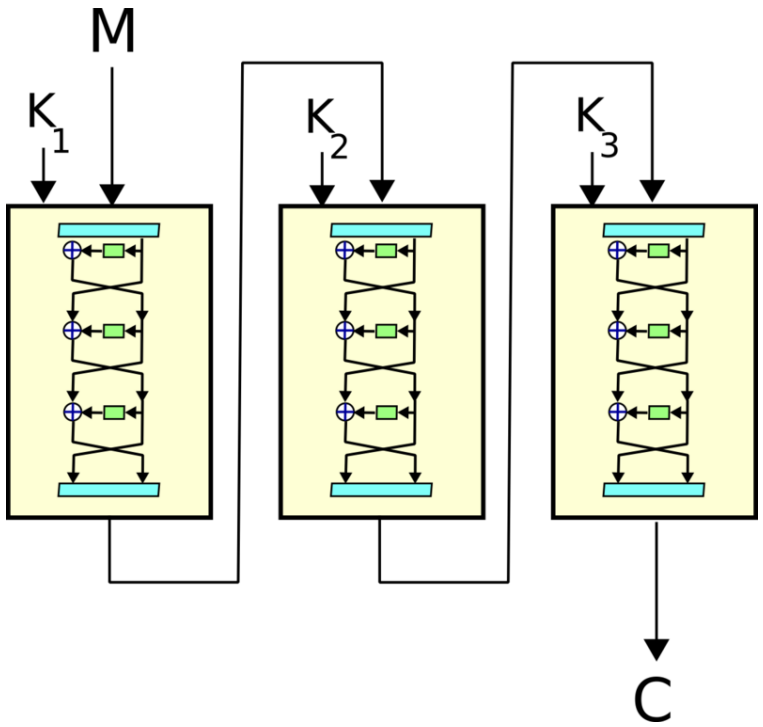
No fim das iterações, os dois blocos G_16 e D_16 são recolados e, em seguida, sujeitos à permuta inicial inversa. O resultado de saída é um texto codificado de 64 bits.

PI-1								
	40	8	48	16	56	24	64	32
	39	7	47	15	55	23	63	31
	38	6	46	14	54	22	62	30
	37	5	45	13	53	21	61	29
	36	4	44	12	52	20	60	28
	35	3	43	11	51	19	59	27
	34	2	42	10	50	18	58	26
	33	1	41	9	49	17	57	25

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Triplo DES - 3DES

É uma simples variação do DES, utilizando-o em três ciframentos sucessivos. O 3DES usa duas (mesma chave na primeira e terceira cifra) ou três chaves únicas, para obter um tamanho de chave de 112 ou 168 bits.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Triplo DES - 3DES

O triplo DES (3DES) foi padronizado pela primeira vez para uso em aplicações financeiras no padrão ANSI X9.17 em 1985.

A principal desvantagem do 3DES é que o algoritmo é relativamente lento em software e usam um tamanho de bloco de 64 bits.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

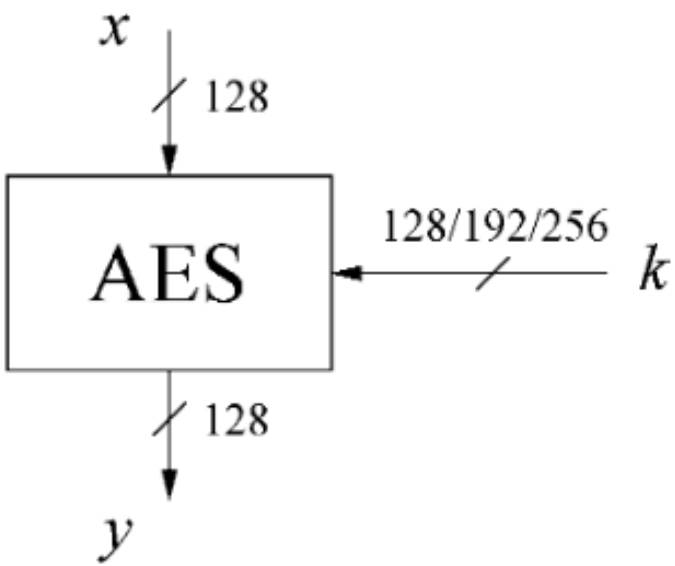
Introdução ao AES

- Em 1997, o NIST (*National Institute of Standards and Technology*) decidiu que o governo Americano precisava de um novo padrão criptográfico. Para isso, eles patrocinaram um concurso de criptografia.
- Este novo algoritmo criptográfico iria substituir o DES (*Data Encryption Standard*), que havia sido quebrado. O 3DES é lento e tem blocos pequenos;
- Pesquisadores do mundo inteiro foram convidados a submeter propostas para um novo padrão, a ser chamado AES (*Advanced Encryption Standard*).
- Em outubro de 2000, o NIST anunciou o algoritmo vitorioso (o Rijndael). O Rijndael, agora AES, se tornou um padrão do Governo dos Estados Unidos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

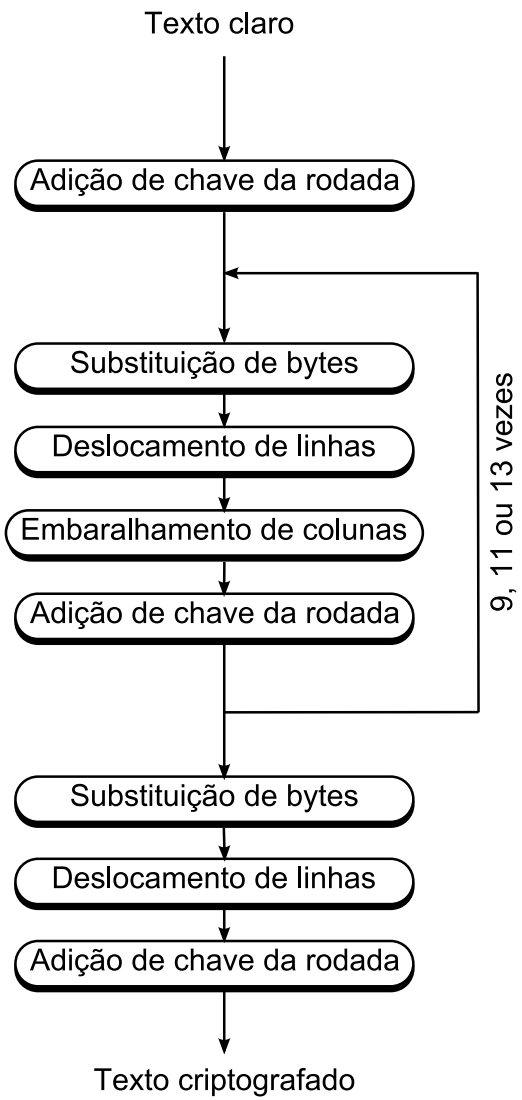
Introdução ao AES

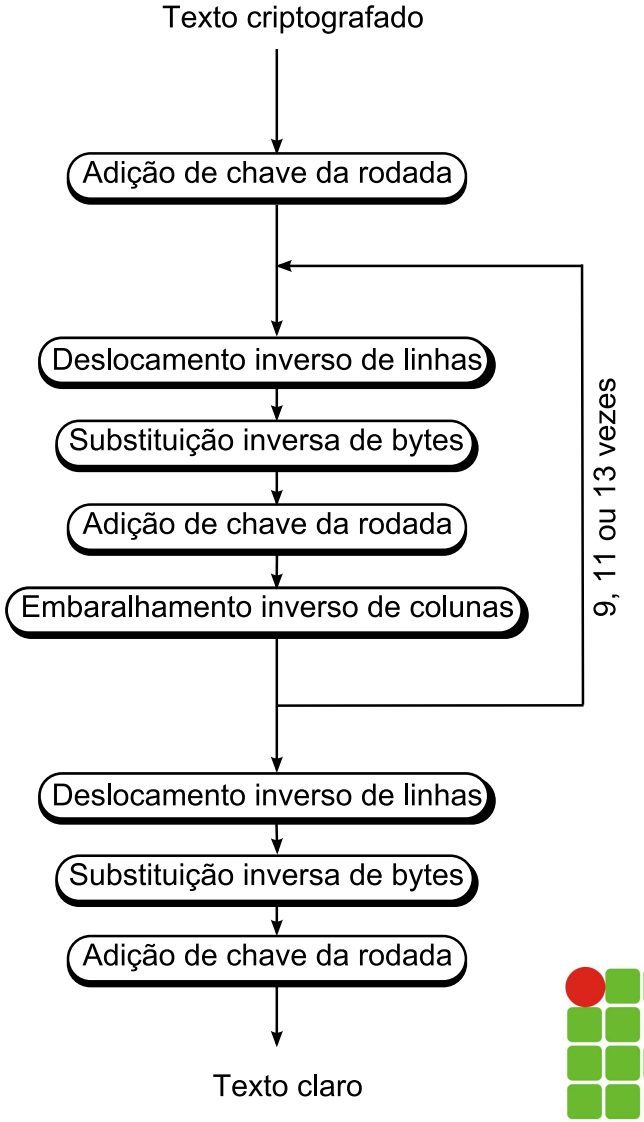
- Atualmente, o AES é um dos algoritmos mais populares usados para criptografia de chave simétrica.
- O AES admite tamanhos de chaves e tamanhos de blocos de 128 *bits*, 192 e 256 *bits*.
- O AES utiliza substituição e permutações emprega várias rodadas (10,11 ou 13 para 128, 192 e 256 *bits*, respectivamente).



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução ao AES





INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução ao AES

- Para criptografar, cada turno do AES (exceto o último) consiste em quatro estágios:
  - Adição de chave da rodada: cada *byte* do estado é combinado com uma subchave (*RoundKey*);
  - Substituição de *bytes*: é uma etapa de substituição, onde cada *byte* é substituído por outro de acordo com uma tabela de referência.
  - Deslocamento de linhas: é uma etapa de transposição, onde cada fileira do estado é deslocada de um determinado número de posições.
  - Embaralhamento de colunas: é uma operação de mescla que opera nas colunas do estado e combina os quatro *bytes* de cada coluna.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução ao AES

Estado

As operações do algoritmo AES são realizadas em uma matriz bidimensional de bytes chamadas de "Estado". Os blocos de 128 bits são copiados em um array organizado em 4 colunas de bytes, cada uma contendo 4 bytes.

Estado

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução ao AES

Adição da chave de rodada

A transformação de adição da chave de rodada (AddRoundKey) consiste em modificar a matriz estado realizando um XOR byte a byte desta com a matriz da subchave da rodada.

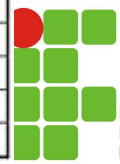
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução ao AES

Substituição de bytes

Consiste em aplicar uma caixa de substituição (S-box) em cada byte da matriz estado. Na tabela faz a intersecção da linha equivalente ao valor dos quatro bits mais significativos do byte e da coluna equivalente ao valor dos quatro bits menos significativos deste mesmo byte. Por exemplo, considere o valor 53.

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

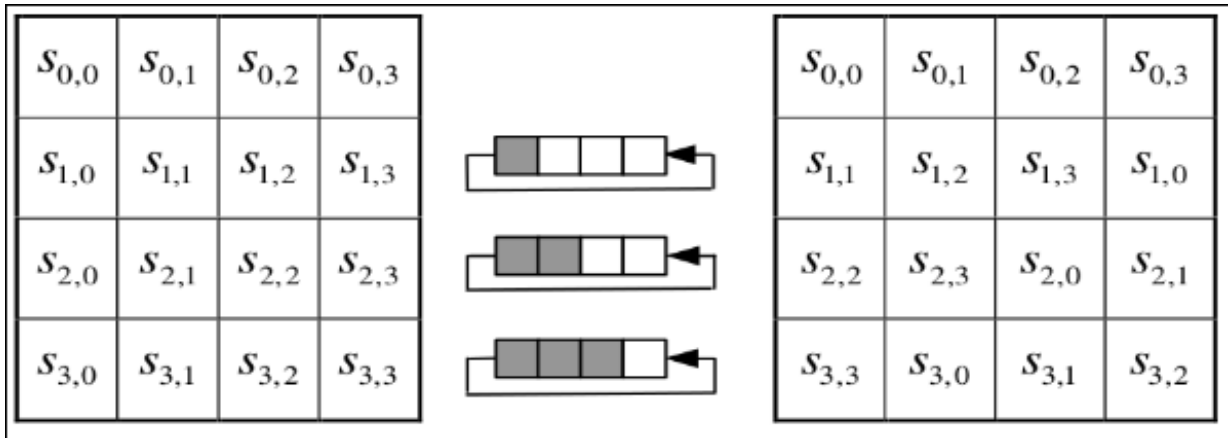


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução ao AES

Deslocamento de linhas

Consiste em uma transposição de deslocamento cíclico dos bytes da matriz estado, onde cada linha é deslocada por um número fixo, de acordo com a linha em questão (0, 1, 2 e 3).

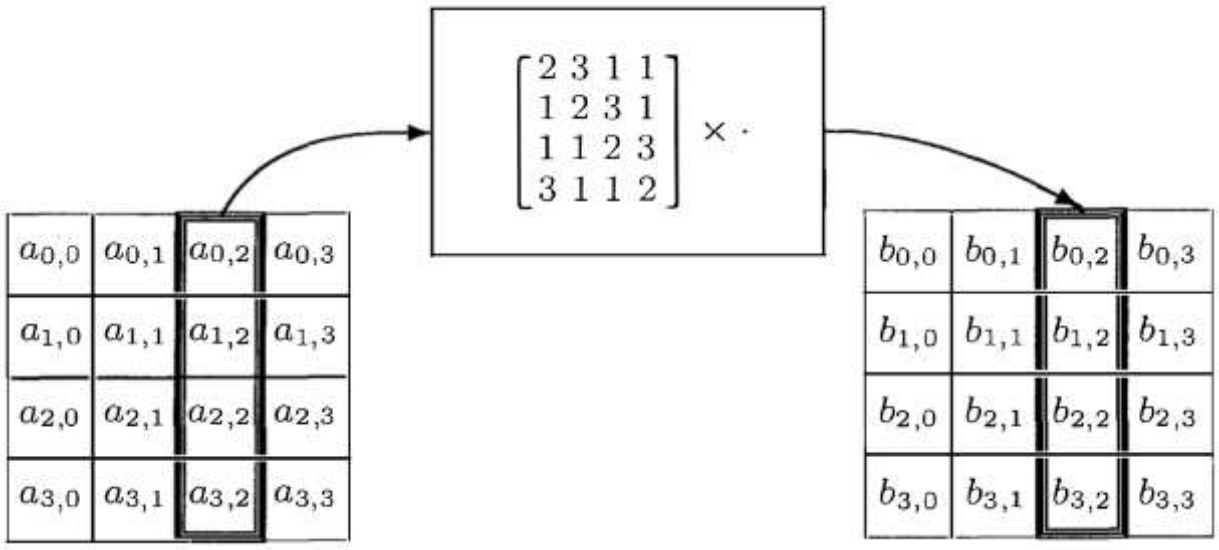


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução ao AES

Embaralhamento de colunas

É uma permutação linear e opera sobre as colunas da matriz de estado. Pode ser representado como uma multiplicação matricial.

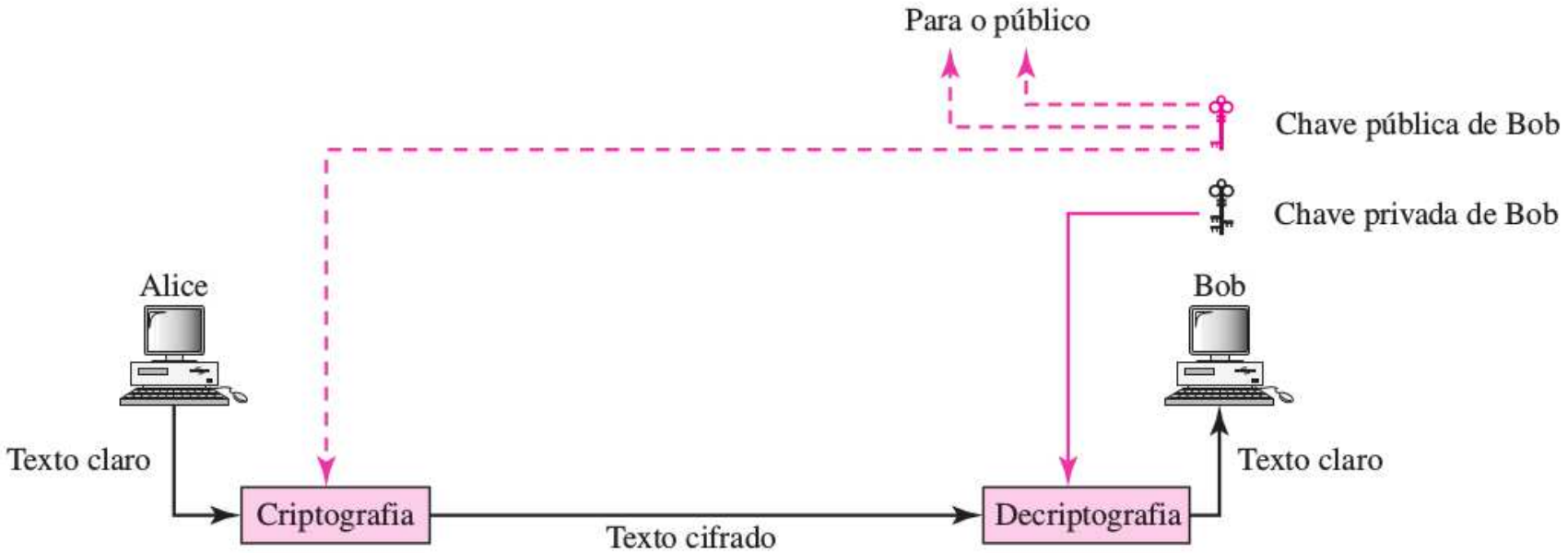


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia

Criptografia de Chave Assimétrica

Existem duas chaves: uma chave privada e uma pública. A chave privada é guardada pelo receptor. Imagine que Alice queira enviar uma mensagem para Bob. Alice usa a chave pública para criptografar a mensagem. Quando Bob recebe a mensagem, a chave privada é utilizada para decriptografá-la.



Criptografia de Chave Pública

Algoritmos de chave pública são baseados em funções matemáticas em vez de em simples operações sobre sequências de bits, como as usadas em algoritmos criptográficos simétricos.

A chave privada é mantida em segredo pelo receptor. Enquanto que a chave pública é distribuída publicamente. Uma restrição, com relação a estas chaves, é que a chave privada não pode ser obtida a partir da chave pública.

A maior desvantagem da criptografia com chaves públicas e a complexidade dos algoritmos que leva a uma quantidade de tempo de processammento relativamente grande.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Pública

Desenvolvido em 1977 (por Ron **R**ivest, **S**hamir e **A**dleman no MIT), vem reinado soberano como a mais amplamente aceita e implementada abordagem da criptografia de chave pública.

Atualmente, um tamanho de chave de 1.024 bits é considerado forte o suficiente para praticamente todas as aplicações.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução ao RSA

Cifração e decifração são realizadas da seguinte forma, para algum bloco de texto às claras M e bloco de texto cifrado C:

$$C = M^e (mod \ \ n)$$

$$M = C^d (mod \ \ n)$$

A chave pública consiste no par (e, n) e a chave privada consiste em (d, n).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução ao RSA

Algoritmo

1. Escolha dois números primos, p e q, onde p $\neq$ q.
2. Calcule $n = p \text{ x } q$ e $z = (p-1)(q-1)$.
3. Escolha um número e tal que $(1 < e < z)$ e (z e e sejam primos entre si).
4. Encontre d de forma que $e \text{ x } d = 1 mod\ z$. Em outras palavras, o resto da divisão de $e \text{ x } d$ por z seja o número 1.

obs.: chamamos números primos entre si (ou coprimos) ao conjunto de números onde o único divisor comum a todos eles é o número 1.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Exemplo:

1. Supondo $p = 17$ e $q = 11$,
2. Calculando

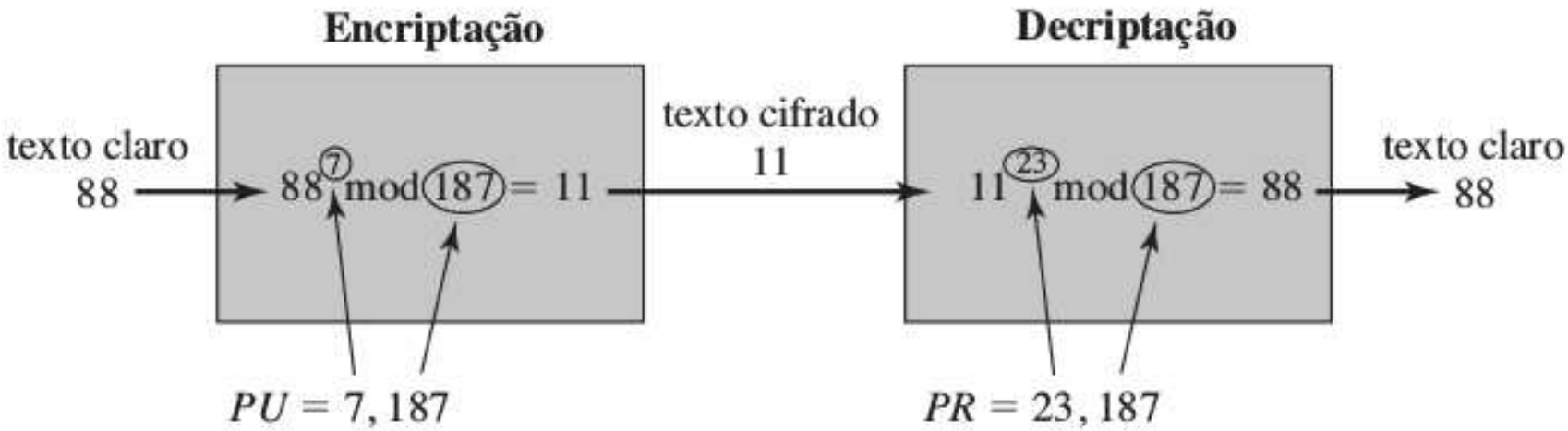
$$\begin{array}{rcl} n & = & p \text{ x } q \\ n & = & 17 \text{ x } 11 \\ n & = & 187 \end{array} \qquad \begin{array}{rcl} z & = & (p-1)(q-1) \\ z & = & (17-1) \text{ x } (11-1) \\ z & = & 16 \text{ x } 10 = 160 \end{array}$$

3. Um valor adequado para e é $e = 7$, visto que $7 > 160$ e são relativamente primos entre si.
4. Escolhe $d = 23$, pois:

$$\begin{array}{rcl} (e \text{ x } d) \; mod \; z & = & 1 \\ (7 \text{ x } 23) \; mod \; 160 & = & 1 \\ 1 & = & 1 \end{array}$$

A chave pública: (7, 187) e a chave privada: (23,187).

Introdução ao RSA



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE