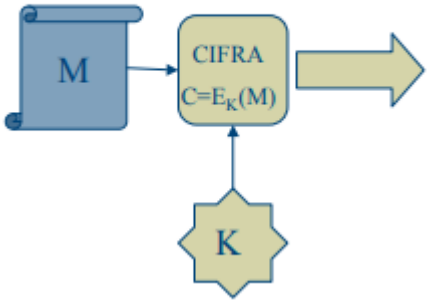
Criptografia

Princípio de Kerckhoff
Para avaliar a segurança de uma técnica criptográfica devemos assumir que esta é do conhecimento do adversário, sendo a segurança da cifra assegurada por um parâmetro chamado chave.

$$C = \mathrm{enc}_K(M)$$



-Adversários
Os adversários podem comprometer a segurança da cifra, fazendo com que esta tenha sido alvo daquilo vulgarmente por ataque.

Existem dois tipos de ataque:

- Passivo: o adversário tem apenas a capacidade de escutar o canal de comunicação(como por exemplo: observar todo o tráfego que circula num canal)
- Ativo: o adversário consegue manipular a informação que circula no canal(alterar/bloquear/injetar mensagens).

-Segurança
Uma técnica criptográfica diz-se segura se nenhum atacante conseguir ter sucesso em atacá-la.
No entanto existem dois tipos de segurança:

- Segurança Absoluta: quando a segurança é estabelecida perante um adversário sem limitações computacionais.No entanto mesmo que um adversário tiver poder computacional infinito, pode ainda assim não conseguir desencriptar uma mensagem(exemplo:cifra one-time-pad).
- Segurança computacional:quando se considera que o adversário dispõe de limitações do poder computacional “realistas”(tempo de processo,capacidade de memória,etc).

Cifras Clássicas

-Cifra de César

Operação da cifra consiste em “um deslocamento” das letras do alfabeto.

Texto limpo:	A	B	C	D	E	F	···	T	U	V	X	W	Y	Z
Criptografia ($K = 6$):	G	H	I	J	K	L	···	Z	A	B	C	D	E	F

O número total de chaves seria 26.

Deve-se portanto considerar também os tamanhos das chaves
Atualmente considera-se que chaves com 280 fornecem um nível mínimo de segurança aceitável

-Cifra de Vignère

Descrição:

- Chave é uma “frase” em que cada letra determina uma substituição
- Tamanho da chave determina número de substituições utilizadas.

-Cifra por Transposição

Considere-se

1	2	3
2	1	3

Para cifrar: AINDAOUTRACIFRA

2	1	3
A	I	N
D	A	O
U	T	R
A	C	I
F	R	A

lê-se a matriz seguindo a ordem da chave...
...resultando seria: IANADOTURCAIRFA

-Combinação de Cifras

Após a análise das cifras simples, faz sentido construir uma cifra complicada combinando várias dessas cifras.
Mas nem sempre faz sentido:

- pode não trazer valor acrescentado(por exemplo, combinando duas cifras por substituição)
- mas há padrões que podem ser vantajosos(por exemplo, intercalando substituições com permutações)

-Cifra One-time-pad

- Generaliza a cifra de Vigenère.
- O tamanho da chave é o mesmo da mensagem a cifrar.
- A chave é completamente aleatória
- As chaves só podem ser usadas numa única operação de cifra.
- Operações de cifra/decifragem são simplesmente o xor com a chave.
- Os problemas devidos à geração e distribuição da chave tornaram a cifra inviável.

Segurança da informação

-Propriedades de Segurança

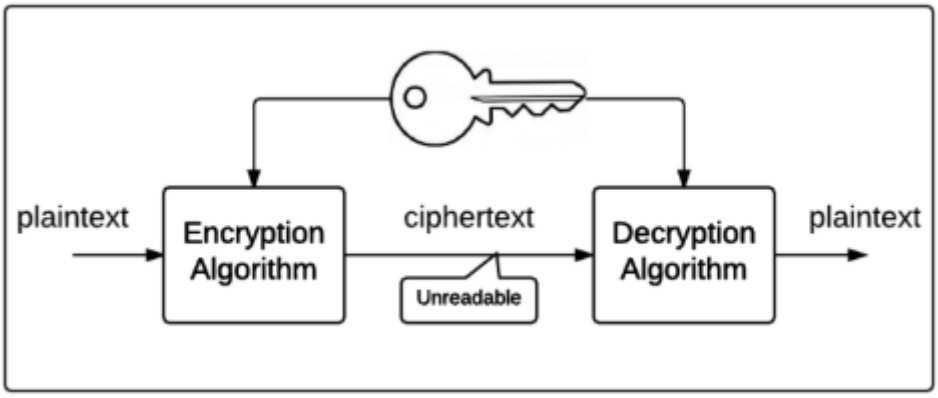
A criptografia é hoje utilizada para fornecer:

- Confidencialidade:garantir que o conteúdo da mensagem só é do conhecimento dos intervenientes legítimos.
- Integridade: garantir que o receptor não aceita mensagens que tenham sido manipuladas.
- Autenticidade: assegurar a “origem ” da mensagem.
- Não repúdio: demonstrar a “origem“ da mensagem
- Anonimato: não fornecer qualquer informação sobre a origem da mensagem
- Identificação: assegurar a “identidade” do interveniente na mensagem

Cifras Simétricas

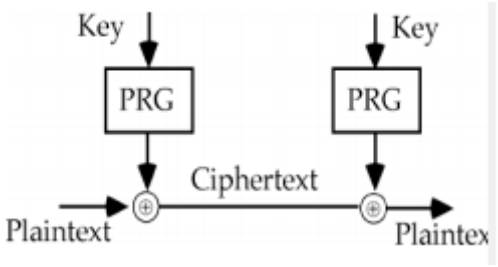
Características:

- Pressupõe um acordo prévio de chaves.
- Operação que tipicamente envolve canais seguros.
- Usa chaves de 40 a 256 bits
- Usa-se a mesma chave encriptar e desencriptar
- Exemplos:RC4,DES,IDEA,AES
- Podem ser de dois tipos: Sequenciais e por blocos.



-Cifras Sequenciais

- A ideia base consiste em aproximar a cifra OneTimePad atraves de um gerador de chaves.



- Processam o texto limpo ”símbolo a símbolo”.
- Tendem a ser muito eficientes e facilmente implementáveis em hardware.
- O processo de geração da sequência de chave tem de ser reprodutível.Logo a sequência é necessariamente cíclica.Diz-se que o período é o comprimento da sequência antes de se começar a repetir. O período deve ser o mais grande possível, sendo sempre maior que a mensagem a transmitir.
- A sequência deve ser pseudo-aleatória e imprevisível.
- São síncronas ou auto-sincronizáveis.

-Cifra One-Time-Pad

- Oferece garantias de confidencialidade.
- Sequência de chave deve ser verdadeiramente aleatória e de comprimento igual à mensagem.
- Chaves nunca devem ser reutilizadas.Um ataque com texto limpo conhecido seria fácil.

-Cifras Síncronas

- A sequência de chave é independente do texto limpo/criptograma
- A perda/inserção de bits no criptograma determinam a “perda de sincronismo”.Ao decifrar, toda a mensagem a partir desse ponto é corrompida.
- Erros(alterações de bits) só alteram a posição correspondente da mensagem original

**********ctr e ofb

-Cifras auto-sincronizáveis

- Cada bit da chave é calculado a partir dos últimos n bits do criptograma.
- Introduz-se um prefixo de n bits aleatórios no texto limpo para permitir sincronização da recepção.

- Ao fim de n bits a decifragem sincroniza(após erro de transmissão ou omissão/inserção de dados no criptograma)
- Vulnerável a ataques por repetição(o adversário pode enviar uma porção do criptogama)

-Cifras por blocos

- Processam blocos de comprimento fixo:Tamanhos típicos para os blocos:64,128 e 256 bits
- Mensagem é partida em blocos do comprimento requerido.

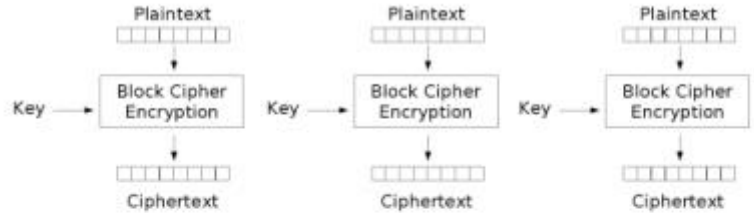
-Confusao e Difusão

De uma cifra por bloco, espera-se que promova:

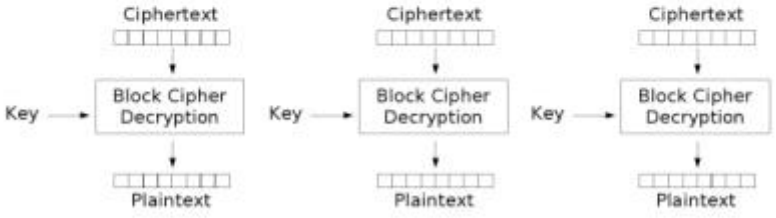
- Difusão:cada bit do texto limpo deve afetar o maior número de bits do criptograma.Desta forma esconde-se as propriedades estatiscas da mensagem.
- Confusao: cada bit do criptograma deve ser uma funcao complexa dos bits do texto limpo.Desta forma dificulta a relacao das propriedades estatístcas do criptograma com as do texto limpo.

-Modos de operação

- Electronic code book(ECB)



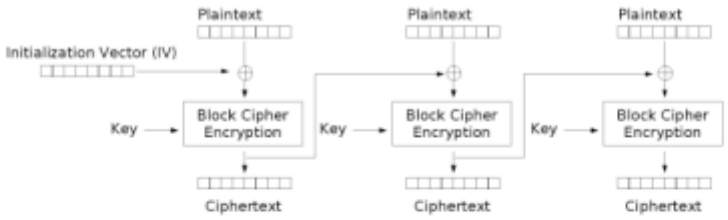
Electronic Codebook (ECB) mode encryption



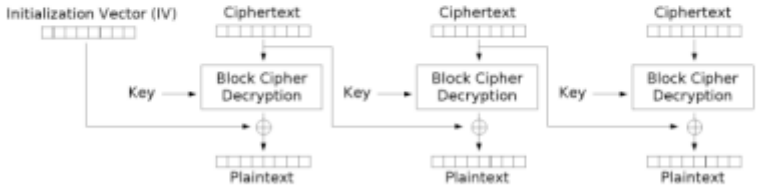
Electronic Codebook (ECB) mode decryption

  - Vulneravel a ataques por repeticao/substituicao,
  - Só deve ser utilizado para cifrar mensagem de um só bloco.
  - Um erro de um bit num bloco do criptograma afecta um só bloco após a decifragem.
  - Uma eventual repetição de blocos é detetavel.

- Cipher Block Chaining(CBC)
    - É utilizado um “vetor de inicialização” (IV) previamente conhecido para iniciar o processo
    - Um erro num bloco do criptograma corrompe dois blocos após a decifragem.(um bloco e um bit)
    - Encadeamento do processo faz depender a operação de cifra de um bloco de todos os que o antecedem

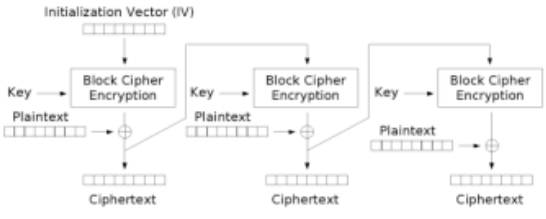


Cipher Block Chaining (CBC) mode encryption

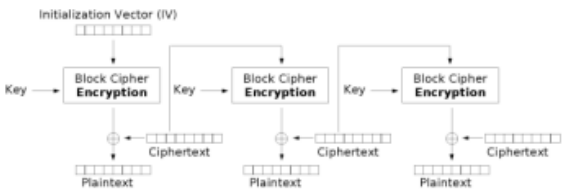


Cipher Block Chaining (CBC) mode decryption

- Cipher FeedBack(CFB)



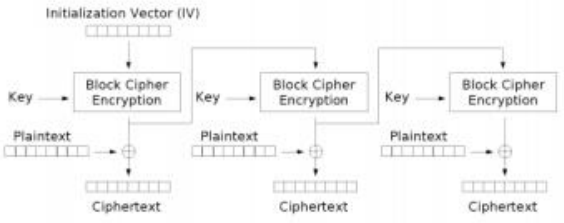
Cipher Feedback (CFB) mode encryption



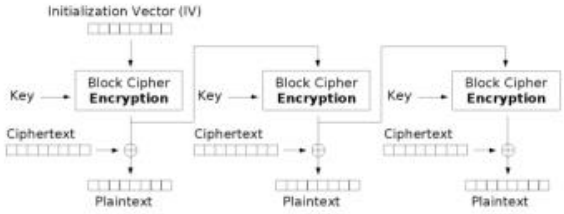
Cipher Feedback (CFB) mode decryption

- Modo que implementa uma cifra sequencial auto-sincronizavel.
- Usa sempre a operação de cifrar.
- IV deve ser unico por cada utilizacao
- Um erro num bit do criptograma afecta o bit respetivo no bloco e todos do bloco seguinte.
- Sequência de chave depende do IV, chave da cifra e de todo o texto limpo já cifrado.

- Output FeedBack(OFB)



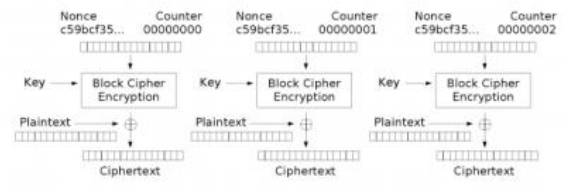
Output Feedback (OFB) mode encryption



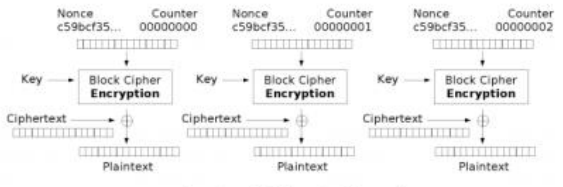
Output Feedback (OFB) mode decryption

- Modo que implementa uma cifra sequencial sincrona com uma cifra por blocos.
- Sequência de chave é obtida iterando a cifra sobre um bloco inicial(iv)
- Sequência de chave é independente da mensagem(pode assim ser processada independentemente de se ter já disponivel a mensagem)
- Erros de bits no criptograma só afectam os respectivos bits na mensagem original

- Counter Mode(CTR)



Counter (CTR) mode encryption



Counter (CTR) mode decryption

- Tal como OFB, simula uma cifra sequencial sincrona(mas agora em counter mode)
- Nonce (IV) e Counter podem ser conjugados de diferentes formas (concatenados,xored,...)
- Único requesito para o Counter é produzir valores distintos para todos os blocos(contador)
- Não impoe dependencia entre processamento de varios blocos(podem por isso ser processados em paralelo)

<u>-Authenticated Encryption</u>
Exemplos:

- EAX(Encrypt-then-mac-translate)
- GCM(counter-mode)
- OCB

-Circuitos de Feistel

Exemplo:o desenho DES(foi desenhado para permitir implementacoes eficientes em hardware.Em contrapartida, exibe algumas operações particularmente ingratas para implementacoes ao nivel do bit)

-Chaves fracas

Dado o mecanismo de escalonamento de chaves do DES(producao das chaves de round a partir da chave inicial),existem algumas chaves com problemas de segurança associados:

- dão origem a chaves todas iguais-chaves fracas
- dão origem a apenas duas subchaves diferentes-chaves semi-fracas
- dão origem a apenas 4 subchaves diferentes.

-Advanced Encryptation Standard(AES)

Nasceu para substituir o DES, concurso NIST.
Tem rounds compostos por 4 camadas.
Todas as operações podem ser realizadas por xor e lookup a tabelas
Adaptado para processadores modernos

-Cifras por blocos vs Cifras sequenciais

- Cifras por blocos são mais complexas.
- As cifras por blocos são mais lentas
- Cifras por blocos protegem a chave(nas sequenciais em cada utilização deve ser utilizada uma chave diferente)
- Unidade de processamento diferente
- As cifras sequenciais não promovem a difusão.

-Padding

Estratégia para completar o último bloco de texto-limpo, sem perder informação sobre o comprimento da mensagem.

Pode ser usado para introduzir aleatoriedade na mensagem.

Funções de sentido único

Podem-se classificar os problemas computacionais como:

- Tratáveis-existe um algoritmo eficiente para a sua resolução.
- Intratáveis--o melhor algoritmo para resolver o problema requer recursos computacionais inviáveis.
- Insolúveis--Não é possível estabelecer um algoritmo para a resolução do problema.

Complexidade

As funções de sentido único são funções que:

- possuam um algoritmo eficiente para o seu cálculo
- não disponham de um algoritmo eficiente que calcule uma sua inversa

-Funções de hash criptográficas

- São funções de sentido único.
- Exibem segurança computacional.
- O objetivo é que mensagens de comprimento aleatório sejam comprimidas para um tamanho fixo.
- Exemplos:MD5,SHA-1,SHA-256,SHA-3

Têm as seguintes propriedades:

- 1ºPre-image resistant: dado um valor de hash h, deverá ser inviável conseguir obter uma mensagem m tal que hash(m)=h
- 2ºPre-image resistant:dado uma mensagem m1, deverá ser inviável obter uma mensagem m2 distinta de m1 tal que hash(m2)=hash(m1)
- Collision resistant: não é viável encontrar mensagens distintas m1 e m2 tais que hash(m1)=hash(m2)

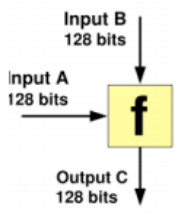
Aplicações:

- Armazenamento de passwords.
- Amplificação da entropia(kdf)
- Componente de outras técnicas como o MAC

Desenho:

O desenho é composto por funções de compressão:

- Estas são funções de sentido único.
- Conhecendo ambas as entradas, é fácil calcular a saída.
- Conhecendo a saída, é difícil calcular qualquer uma das entradas
- Conhecendo a saída, e uma das entradas, é difícil calcular outra.
- Deve também ser resistentes a colisões.
- Podem ser construídas a partir de cifras por blocos



MD5:

- Tamanho do contra-dominio:128 bit
- Processa a mensagem em blocos de 512 bits.
- Opera em rounds
- É desaconselhado o seu uso devido a terem-se encontrado colisões.

SHA-1

- Tamanho do contra-dominio:160 bit
- Otimizada para arquiteturas big-endian

SHA-3

- Utiliza sponge-construction(permite processar um input e gerar um output de tamanho aleatório)
- tamanho do contra-dominio:224/256/384/512 bits

-Message Authentication Codes(MAC)

- As funções de hash, por isso só, não garantem nem a integridade nem a autenticidade (mas quando utilizadas com uma cifra já permitem estabelecer essas propriedades)
- Um código de autenticação (MAC), pode ser entendido como uma função de hash com segredo" e visa garantir essas propriedades.

A forma mais simples de construir um MAC é combinar uma função de hash com um segredo(de forma apropriada).Chama-se a isso HMAC.

-MACs derivados de cifras por blocos

O último bloco de criptograma do modo cbc pode ser utilizado como um MAC(cbc-mac)
Modos:EAX,GCM,OCB

-PBKDF

Por vezes há necessidade de construir uma chave apropriada para uma dada técnica a partir de chaves fracas (e.g. passwords ou passphrases).

O principal problema é ficar-se vulnerável a ataques de dicionário - o adversário pode "catalogar" todo o espaço de chaves.

Estratégias para dificultar esses ataques:

- Considerar factores aleatórios (designados por salt, ou IV). Assim procura-se impedir a pré-computação do dicionário. Na sua forma mais simples, o salt é concatenado com o segredo.
- Aumentar o "peso computacional" da função de derivação da chave. Assim dificulta-se a realização de ataques em tempo real.

No PBKDF1, o segredo obtido com o mesmo tamanho do resultado da função hash
No PBKDF2, o segredo tem comprimento diferente do resultado da função de hash
SCrypt é um kdf especialmente desenhado para resistir a ataques. A estratégia passa por forçar a utilização de uma quantidade de memoria intermedia considerável.

DES CRYPT<MD5<MD5
CRYPT<PBKDF2<BCRYPT<SCRYPT<PBKDF2<BCRYPT<SCRYPT