3. Criptografia

3.3. Um pouco mais sobre Criptografia

›Ataques e modelos de segurança

Um pouco sobre ataques...

- Ataques criptanalíticos
  - O adversário tenta quebrar o algoritmo criptográfico
  - Busca de "fraquezas" no algoritmo de encriptação
- Ataques a protocolos
  - O adversário busca um ponto fraco na forma de uso da criptografia
  - Exemplos:
    - premissa mal estabelecida
    - objetivo de segurança mal determinado
    - uso de uma primitiva que deveria ser aplicada a objetivo diverso
- Ataques a implementações
- Ataques a sistemas/procedimentos

Tipos de ataques criptanalíticos

- Ataques são classificados de acordo com a postura do oponente diante do esquema
  - possivelmente ele apenas terá acesso a um conjunto de mensagens-cifradas
  - talvez ele conheça alguns pares de mensagem-plana e mensagem-cifrada correspondente
  - e talvez possa, ainda, escolher um conjunto mensagens planas e obter as mensagens cifradas correspondentes (ou vice-versa)
- O que determinará a postura do oponente será: a quais elementos do esquema ele tem acesso?
  - apenas ao canal de comunicação?
  - à "máquina" de encriptação?
  - à "máquina" de decriptação?

Tipos de ataques criptanalíticos

- Somente mensagens cifradas (ciphertext only)
  - O adversário tem acesso apenas a um conjunto de mensagens cifradas
- Mensagens planas conhecidas (known plaintext)
  - O adversário tem acesso a pares de mensagens planas e mensagens cifradas correspondentes
- Mensagem escolhida (chosen text)
  - Escolhe mensagem plana e obtém mensagem cifrada correspondente (chosen plaintext)
  - Escolhe mensagem cifrada e obtém mensagem plana correspondente (chosen plaintext)

Criptografia e protocolos criptográficos

- Criptografia é uma ferramenta matemática para prover segurança à informação
- Protocolos determinam de que modo primitivas criptográficas serão usadas em uma rede de comunicação
  - Estabelecimento e distribuição de chaves
  - Passos para o estabelecimento de comunicação
  - Formato de pacotes de informação
  - Etc.

Modelos de segurança

- Segurança incondicional
  - Não importa quanto poder computacional esteja disponível, a cifra não pode ser quebrada
  - A mensagem cifrada contém informação insuficiente para, por si só, determinar a mensagem plana correspondente
- Segurança computacional
  - Dados recursos computacionais limitados a cifra não pode ser quebrada
  - Exemplo: o tempo necessário, usando o mais potente computador disponível e os algoritmos atualmente conhecidos, é maior que a idade do universo

›Cifras e técnicas clássicas

Técnicas clássicas

- As cifras clássicas (até a década de 1970) são de chave simétrica
- Ou seja, a transformação de encriptação e sua inversa são "facilmente" determináveis, uma a partir da outra
- Dois componentes básicos estão presentes na maioria das cifras clássicas
  - operações de substituição, transposição e mistura
- Tais operações ainda são blocos básicos da construção de muitos algoritmos de chave simétrica usados nos dias de hoje

Técnicas clássicas

- Substituição
  - Símbolos / conjuntos de símbolos substituídos por símbolos / conjuntos de símbolos
- Transposição
  - Símbolos / conjuntos de símbolos rearranjados em ordem diferente
- Mistura
  - Operações lógicas (XOR) entre chave e mensagem
- Saídas de diferentes cifras podem ser concatenadas para se construir cifras mais complexas (cifra produto)

Brevíssimo histórico da criptografia

- Cifras antigas
  - Tumba de Khnumhotep II
  - Substituição deliberada de alguns símbolos
  - Transformação da escrita com diversos possíveis objetivos
    - Ex.: criar aura de mistério
  - Mais antigo texto conhecido contendo modificação deliberada de linguagem

Cifra Scytale

- Cifrador espartano de transposição (400AC)
- Fita de papel era enrolada em uma vareta
- Mensagem escrita enquanto a fita está enrolada; depois o papel é removido, ficando a fita com uma seqüência de letras aparentemente aleatória
- A chave é definida pela circunferência da vareta e a espessura do papel

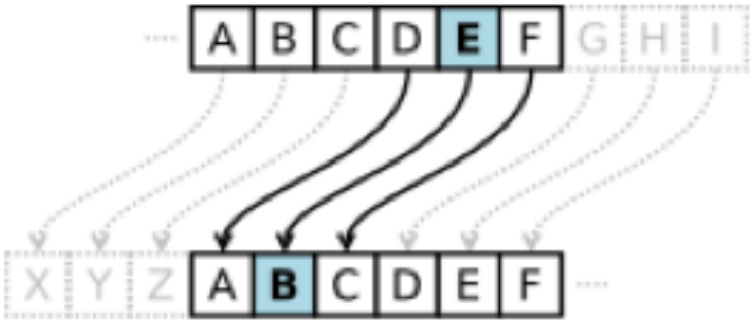
	A	J	U	D	E	
	M	E	S	T	O	
	U	S	O	B	A	
	T	A	Q	U	E	

Brevíssimo histórico da criptografia

- Cifras antigas (esteganografia)
  - Heródoto registra o uso de esteganografia pelos persas (400 AC)
    - Damaratus avisa gregos sobre Xerxes (cera sobre madeira)
    - Histaiaeus envia mensagem a Aristagoras de Miletus (tatuagem no couro cabeludo)

Brevíssimo histórico da criptografia

- Cifras antigas
  - Cifra de substituição supostamente utilizada por Júlio César (100 AC)
  - Basicamente, um "deslocamento" do alfabeto



Brevíssimo histórico da criptografia

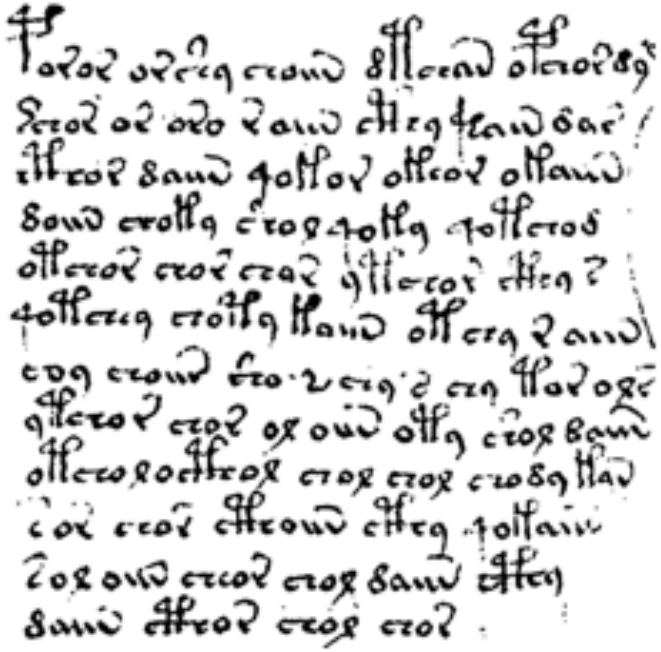
- Al-Kindi estuda estatísticas das linguagens e desenvolve primeiras técnicas de criptanálise (séc. IX)
- O "tratado" de criptografia foi redescoberto em 1987, em Istambul
  - Chama-se "Manuscrito sobre 'deciframento' de mensagens criptografadas"

Brevíssimo histórico da criptografia

- Ahmad al-Qalqashandi (1355-1418 DC)
- Escreve enciclopédia (*Subh al-a 'sha*, 14 volumes) com seção dedicada à criptografia (1412 DC)

Brevíssimo histórico da criptografia

- Manuscrito de Voynich (1450-1520 DC)



Brevíssimo histórico da criptografia

- Cifra Leon Alberti (1466 DC)

Brevíssimo histórico da criptografia

- Livro de Vigenère sobre cifras (1585)
  - Traicte de Chiffres
  - Idéia baseada em Giovan Batista Belaso

Cilindro de Jefferson

Cilindro de Jefferson

- Desenvolvido em 1795
  - 26 discos, cada um com uma ordem aleatória do alfabeto
  - Os discos podem ser reordenados
    - Emissor e receptor "combinam" uma ordenação
  - Emissor gira os discos de maneira a formar a mensagem plana em uma linha
    - Ele transmite a seqüência de caracteres de outra linha
  - Receptor gira os discos de maneira a formar a mensagem cifrada em uma linha
    - A mensagem plana irá aparecer em outra linha

Disco de Wheatstone

- Disco de Wheatstone
  - Originalmente inventado por Wadsworth em 1817
  - Desenvolvido por Wheatstone em 1860
  - Dois discos concêntricos geral uma cifra polialfabética

Urkryptografen: versão do disco de Wheatstone usado pelo exército dinamarquês de 1936 a 1948

Brevíssimo histórico da criptografia

- Kerchhoff e as leis da criptografia (1883)

JOURNAL

DES

SCIENCES MILITAIRES

DES

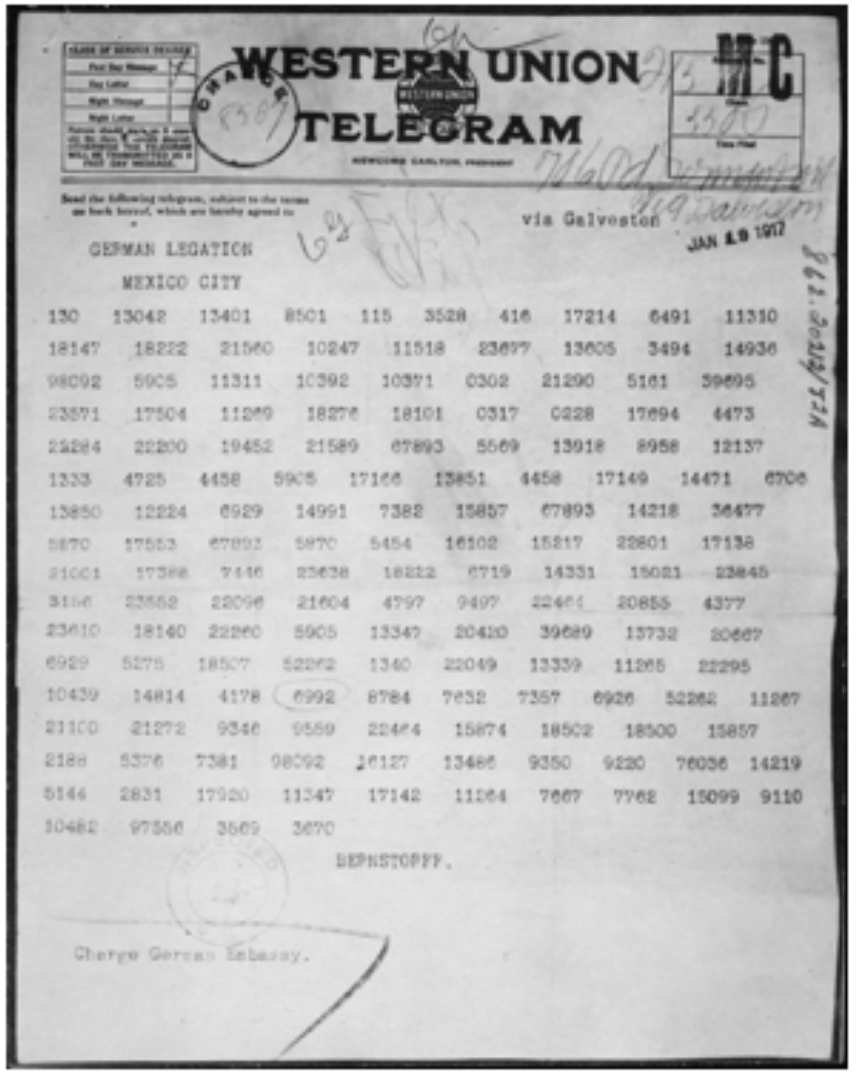
ARMÉES DE TERRE ET DE MER,

PUBLIÉ

SUR LES DOCUMENTS FOURNIS PAR LES OFFICIERS DES ARMÉES FRANÇAISES ET ÉTRANGÈRES,

Telegrama de Zimmerman

› Entrada dos EUA na I Guerra



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23697 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 16222 6719 14331 15021 23845
3156 22552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

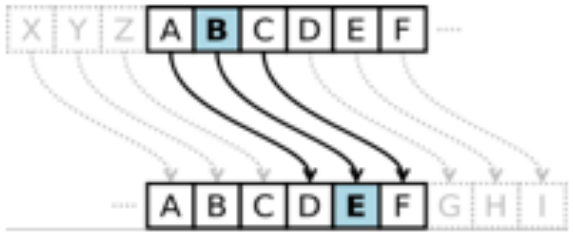
Enigma

- Importante classe de máquinas cifradoras
- Bastante utilizada durante a Segunda Guerra Mundial
- Discos contendo conexões internas gerando substituições com alfabetos modificados continuamente

Entendendo melhor as cifras ”básicas”

Cifra de César

- Supostamente usada por Júlio César
- Substitui cada letra numa mensagem pela *k*-ésima letra seguinte no alfabeto
  - Originalmente, k=3
- Exemplo
  - Mensagem cifrada: `YLP YL YHQFL`
  - Mensagem plana: `VIM VI VENCI`
- Podemos descrever a cifra da seguinte forma
  - Encriptação $E_K(i) = i + k \bmod 26$
  - Decriptação $D_K(i) = i - k \bmod 26$



Criptanálise da cifra de César

- Apenas 26 possíveis cifras (na verdade, 25...)
  - A é mapeado para A,B,...,Z
- Ataque por força bruta
  - Basta tentar cada uma das chaves
  - É necessário saber reconhecer mensagens planas

Cifra monoalfabética

- Em vez de "deslocar" o alfabeto (cifra de César), podemos "embaralhá-lo"
- Cada letra de mensagem plana é mapeada para uma letra na mensagem cifrada correspondente
- Chave de tamanho 26 letras
- Exemplo

```
Alfabeto:     ABCDEFGHIJKLMNOPQRSTUVWXYZ
Chave:        QAZWSXEDCRFVTGBYHNUJMIKOLP
Msg Plana:    ATACARAMANHAASDUASDATARDE
Msg Cifrada:  QJQZQNQTQGDQQUWMQUWQJQNWS
```

Segurança da cifra monoalfabética

- Agora temos um total de 26! chaves: 403291461126605635584000000
- Com um espaço de chaves tão grande, poder-se-ia pensar que a cifra é segura
- ERRADO
- O problema são as características das linguagens naturais

Redundância de linguagens naturais

- Linguagens naturais (humanas) são **redundantes**
- As letras não aparecem todas com a mesma freqüencia
- Na língua portuguesa, **A** é a letra mais freqüente
  - Outras letras frequentes: E, O, S, D, R
- Outras letras são mais raras
  - Exemplo: Z,J,H,Q,X
- Também existem tabelas de freqüências para pares e triplas de letras

“Diluindo” padrões estatísticos

- Cada símbolo é mapeado para um par de símbolos
- Mapeamento não-determinístico
- Símbolos mais freqüentes -> maior número de possíveis mapeamentos
- Exemplo
  - G mapeado para algum par em {AF,RN,SU,OH,NR,OG}
  - X mapeado para algum par em {RJ,OS}
- Problemas
  - aumenta tamanho da mensagem
  - não destroi todas as estatísticas

Auto-chave

- Idéia proposta por Vigenère
  - Tentativa de tornar a chave tão longa quanto a mensagem
- Palavra-chave é prefixada à mensagem, que passa a funcionar como chave
  - Conhecendo-se a palavra-chave, decifra-se o início do texto plano
  - Cada caractere decriptado compõe mais um caractere da chave
- Ainda mantém características de freqüência que podem ser exploradas
- Ex.: plavra-chave *segredo*

Chave:	`SEGREDOFOMOSDESCOBERTOSBATEREMR`
Texto plano:	`FOMOSDESCOBERTOSBATEREMRETIRADA`
Texto cifrado:	`XSSFWGSXQAPWUXGUPBXVKSESEMMIEPR`

Cifras de transposição

- Buscam ocultar o conteúdo da mensagem através do rearranjo da ordem dos caracteres
- Mantém a distribuição de freqüência de caracteres inalterada
- Apresentaremos algumas cifras de transposição clássicas

Cifra Rail Fence

- Escreva as letras da mensagem em diagonais passando por diversas linhas
- Então, leia as letras linha por linha
- Exemplo: `ENCONTRE-ME NO FRONT`

```
E C N R M N F O T
 N O T E E O R N
```

- Nos dá a seguinte mensagem cifrada

```
E C N R M N F O T N O T E E O R N
```

Cifra de transposição de linhas

- Escreva a mensagem em linhas com determinado número de colunas
- Reordene as colunas de acordo com uma chave
- Leia as letras coluna por coluna

```
Chave:          3 4 2 1 5 6 7
Msg Plana:      A T A C A R A
                M A N H A A S
                D U A S D A T
                A R D E X Y Z
Msg. Cifrada: ANADCHSETAURAMDAAADXRAAYASTZ
```

Composição de cifras (produto)

- Cifras que usam apenas substituições ou transposições são facilmente quebráveis
  - Motivo principal: características estatísticas das linguagens naturais
- Investiguemos a aplicação de diversas cifras, em seqüência
  - Duas substituições seguidas equivalem a uma nova substituição
  - Duas transposições seguidas equivalem a uma nova transposição
  - Uma substituição seguida de transposição determinam uma cifra mais complexa
- Essa é a ponte entre as cifras clássicas e as cifras modernas

Formalizando a notação

- Domínio e codomínio de encriptação
  - $\mathcal{A}$: conjunto finito denominado *alfabeto de definição*.
    - Usaremos $\mathcal{A}_M$ e $\mathcal{A}_C$ caso o conjuntos de símbolos das mensagens planas seja diferente do conjunto de símbolos das mensagens cifradas.
  - $\mathcal{M}$: conjunto denominado *espaço das mensagens-planas*. $\mathcal{M}$ consiste de seqüências de símbolos do alfabeto de definição. Um elemento de $\mathcal{M}$ e chamado *mensagem-plana*.
  - $\mathcal{C}$: conjunto denominado *espaço das mensagens-cifradas*. $\mathcal{C}$ consiste de seqüências de símbolos do alfabeto de definição, o qual pode ser diferente do alfabeto de definição de $\mathcal{M}$. Um elemento de $\mathcal{C}$ é chamado *mensagem-cifrada*.

Formalizando a notação

- Transformações de encriptação e decriptação
  - $\mathcal{K}$ denota um conjunto chamado *espaço das chaves*. Um elemento de $\mathcal{K}$ é chamado *chave*.
    - Usaremos $\mathcal{K}_M$ e $\mathcal{K}_C$ caso o conjuntos de símbolos das mensagens planas seja diferente do conjunto de símbolos das mensagens cifradas.
  - Cada elemento $e \in \mathcal{K}$ detemina uma bijeção E_e de $\mathcal{M}$ para $\mathcal{C}$ chamada *função* ou *transformação de encriptação*.
  - Cada elemento $d \in \mathcal{K}$ detemina uma bijeção D_d de $\mathcal{C}$ para $\mathcal{M}$ chamada *função* ou *transformação de decriptação*.
  - Aplicar a transformação E_e a uma mensagem $m \in \mathcal{M}$ significa *encriptar* ou *criptografar* m.
  - Aplicar a transformação D_d a uma mensagem $c \in \mathcal{C}$ significa *decriptar* ou *decriptografar* c.

Formalizando a notação

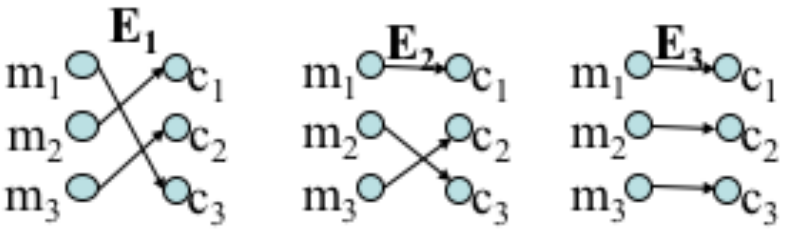
- *Esquema criptográfico* ou *cifra*
  - Conjunto $\mathcal{K}$ de chaves
  - Conjunto $\{E_e : e \in \mathcal{K}\}$ de transformações de encriptação
  - Conjunto $\{D_d : e \in \mathcal{K}\}$ de transformações de decriptação
  - Para cada chave $e \in \mathcal{K}$, existe uma única chave $d \in \mathcal{K}$ tal que $D_d = E_e^{-1}$
    - Ou seja, $D_d(E_e(m)) = m$ para toda mensagem $m \in \mathcal{M}$.

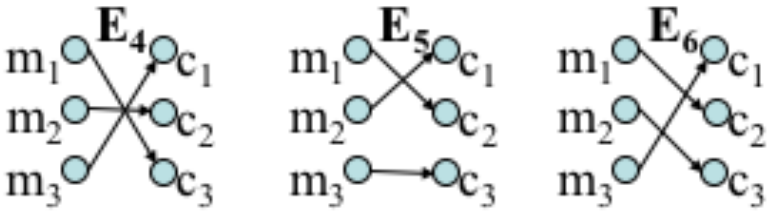
Formalizando a notação

- Construir uma cifra significa
  - selecionar os conjuntos $\mathcal{M}$, $\mathcal{C}$, e $\mathcal{K}$;
  - determinar o conjunto de transformações de encriptação $\{E_e: e \in \mathcal{K}\}$; e
  - determinar o conjunto de transformações de decriptação $\{D_d: e \in \mathcal{K}\}$ correspondentes
  - Obs.: como $E_e^{-1} = D_d$, então $\mathcal{M}$ e $\mathcal{C}$ devem ter a mesma cardinalidade

Exemplo

- $\mathcal{M} = \{m_1, m_2, m_3\}$
- $\mathcal{C} = \{c_1, c_2, c_3\}$
- $\mathcal{K} = \{1,2,3,4,5,6\}$
  - são 3!=6 bijeções de $\mathcal{M}$ a $\mathcal{C}$
- Cada chave i determina uma transformação de encriptação E_i

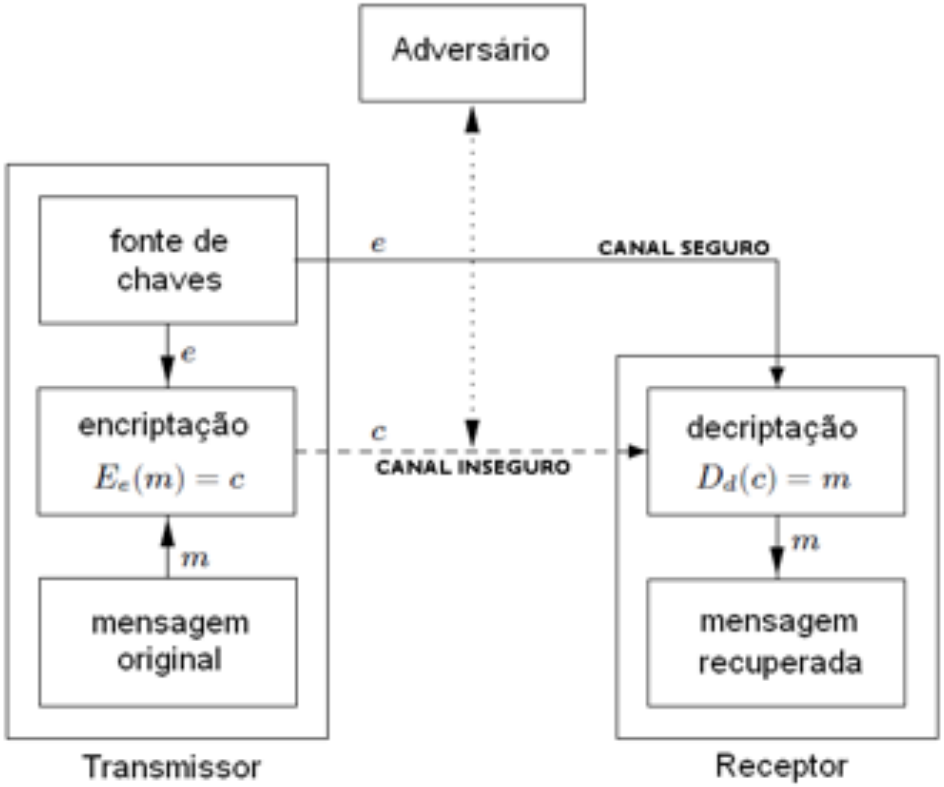




A chave e as transformações de encriptação e decriptação

- Como dissemos, uma chave determina funções de encriptação e decriptação
- Intuição importante: não necessariamente é fácil calcular essas funções a partir da chave
  - Para casos patológicos, a pode ser inviável encriptar a partir da chave

Confidencialidade usando cifras de chave simétrica



›Cifras modernas de chave simétrica

Cifras de stream

- Processa a mensagem caractere a caractere (ou bit a bit), como uma stream
- Ex.: Cifra de Vernam
  - Vernam cipher
  - Descrita por Vernam, trabalhando para a AT&T em 1917
  - Simplesmente soma (XOR) os bits da mensagem a bits (pseudo-) aleatórios de uma chave
  - Incondicionalmente seguro, se a chave é realmente aleatória e desconhecida
    - São necessários tantos bits quanto aqueles da mensagem (pouco prático)

Cifras de bloco

- Cifras de bloco quebram a mensagem e a encriptam bloco a bloco
- É como uma substituição de caracteres “longos” (64-bits ou mais)
- A maioria das cifras modernas que estudaremos são deste tipo

Princípios das cifras de bloco

- Cifras de bloco funcionam como uma grande substituição
  - Para blocos de 64 bits, cada uma das 2^{64} mensagens planas é levada, de forma bijetiva, em uma de 2^{64} mensagens cifradas
- Construir tal tabelas de substituições seria impraticável
- Muitos dos cifradores de bloco modernos são baseados na chamada Estrutura de Cifra de Feistel
- Utilizam-se blocos menores de construção
- Então, usa-se a idéia de composição de cifras

Cifras de bloco iteradas

- Envolve a repetição de funções internas chamadas rounds
- São parâmetros da cifra
  - Número de rounds
  - O tamanho do bloco
  - O tamanho da chave, de onde serão tiradas as subchaves de cada round
- Cada round deve ser uma função bijetiva

Estrutura das cifras de Feistel

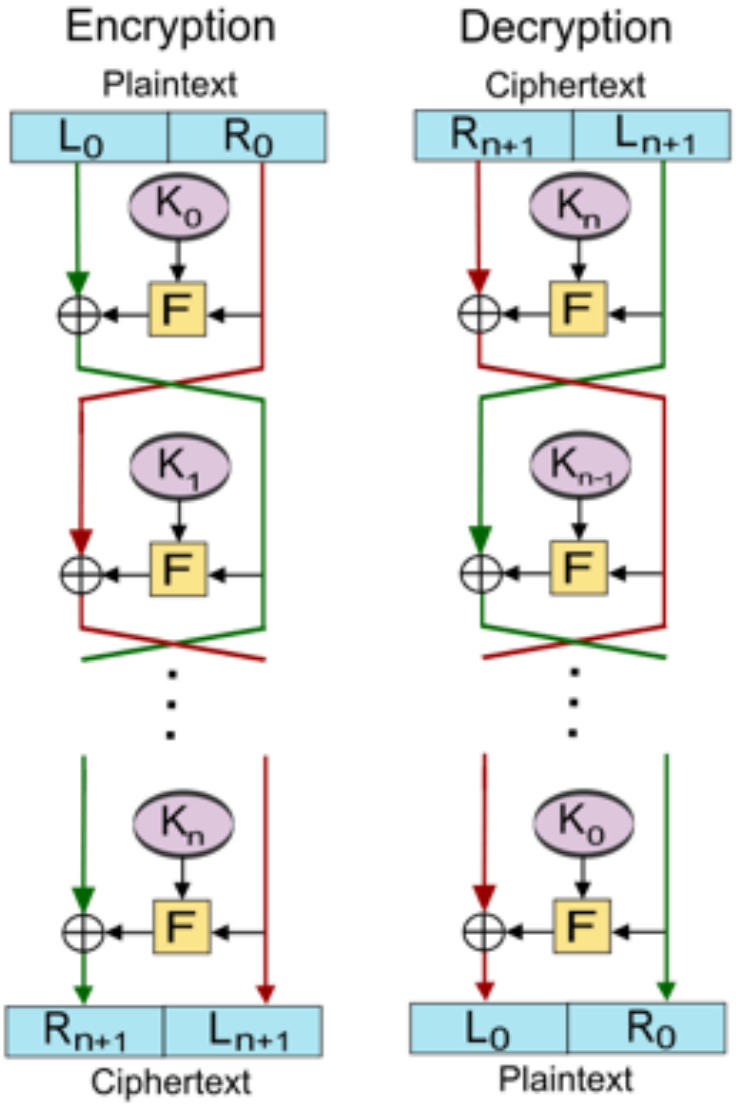
- Desenvolvida por Horst Feistel
- Particiona o bloco de entrada em duas partes de mesmo tamanho
- Processa em rounds nos quais
  - Aplica substituição, na metade esquerda, baseada no conteúdo da metade direita e em subchave derivada da chave
  - Então, permuta as duas partes
- Formalmente:
  - $L_i = R_{i-1},\ R_i = L_{i-1} \oplus f(R_{i-1},K_i)$

Decriptação da Cifra de Feistel

- Tipicamente, $r \geq 3$ rounds
- Ordena a saída como (R_r, L_r)
- Decriptação: apenas aplicar os rounds na ordem reversa

Estrutura da cifra de Feistel

- Cifras de Feistel ou modificações da cifra de Feistel: Blowfish, Camellia, CAST-128, DES, FEAL, ICE, KASUMI, LOKI97, Lucifer, MARS, MAGENTA, MISTY1, RC5, TEA, Triple DES,Twofish, XTEA, GOST 28147-89
- Generalizações da cifra de Feistel: CAST-256, MacGuffin, RC2, RC6, Skipjack, SMS4, CLEFIA



Data Encryption Standard (DES)

- Cifra de bloco por muito tempo mais usada no mundo
  - Após ter recomendação retirada, passou a ser usada na forma do triple-DES (que está para ser aposentado tb=)
- Pode-se dizer que é a mais estudada e conhecida
- Adotada em 1977 pelo NBS (agora NIST)
  - FIPS PUB 46
- Encripta blocos de 64 bits usando chaves de 56 bits
- Já não pode ser considerada segura

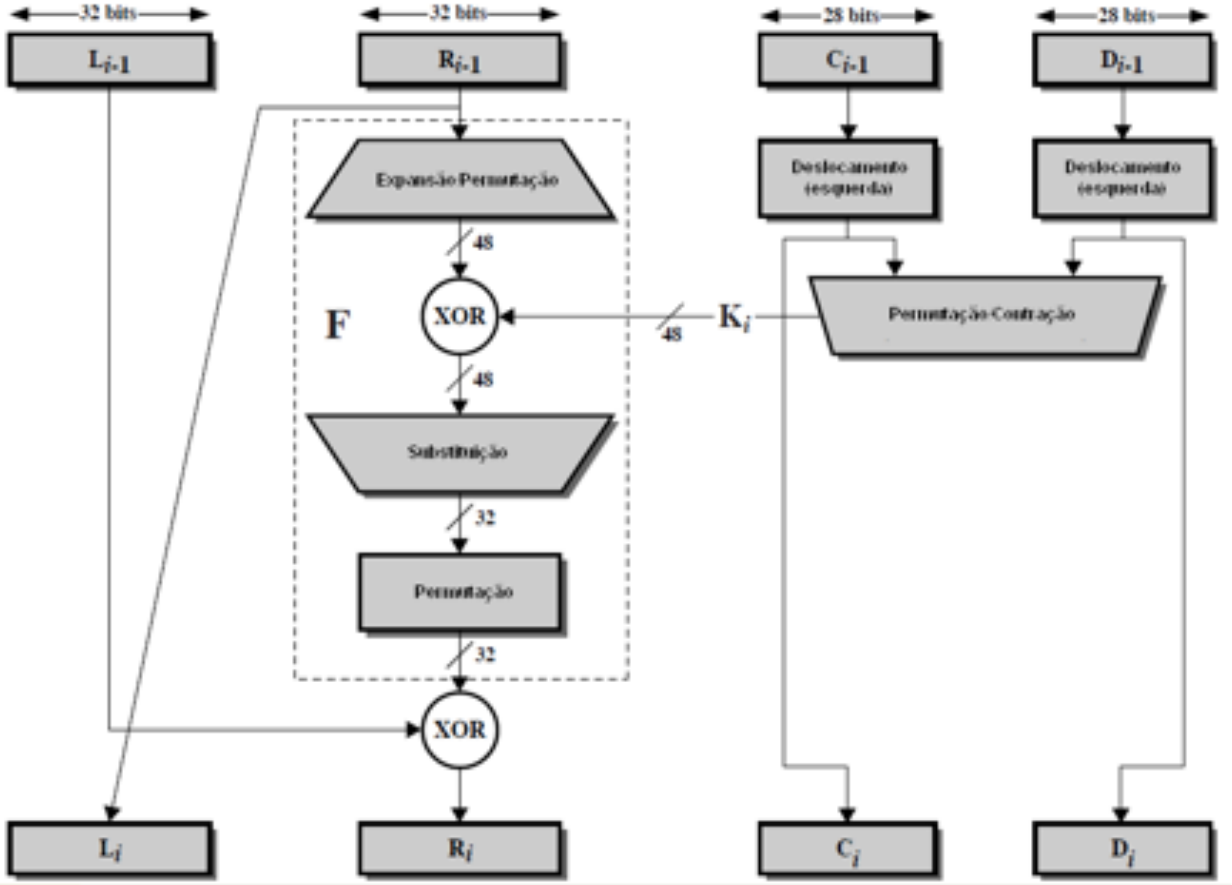
História do DES

- IBM desenvolve a cifra Lucifer em 1971
  - Equipe liderada por Feistel
  - Bloco de 48, 32 or 128 bits
  - Chave de 48, 64 or 128 bits
- Em 1973, o NBS solicitou propostas para um novo padrão nacional de cifras
- A IBM submeteu uma versão revisada do Lucifer, que finalmente seria aceita como DES

Estrutura do DES

- Tamanho de bloco: 64 bits
- Tamanho de chave: 56 bits
  - Na verdade, são 64 bits, com 8 de paridade
- Número de estágios: 16 rounds
  - 16 subchaves de 48 bits são geradas
  - Cada round é um round de Feistel:
    - Li = Ri-1;
    - Ri = Li-1 ⊕ f(Ri-1,Ki), onde
      f(Ri-1,Ki) = P(S(E(Ri-1)⊕Ki))

Round do DES


32 bits
32 bits
28 bits
28 bits
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
Expansão-Permutação
Deslocamento (esquerda)
Deslocamento (esquerda)
48
F
XOR
48
K_i
Permutação-Contração
48
Substituição
32
Permutação
32
XOR
L_i
R_i
C_i
D_i

Busca exaustiva de chave

- Uma chave de tamanho fixo determina um limite superior para a segurança de um cifrador (busca exaustiva de chave)
- Considere uma cifra de blocos de n bits com espaço de chaves de tamanho k
- Dado um pequeno número de pares mensagem plana /mensagem cifrada, a chave pode ser encontrada com tempo esperado de $2^k/2=2^{k-1}$ operações
  - Basta decriptar a mensagem cifrada e comparar com a mensagem plana disponível
  - Pode ser necessário mais de um par, dependendo do tamanho relativo entre n e k

Busca exaustiva – texto com redundância

- Se é conhecida alguma redundância nas mensagens planas, o número de mensagens cifradas pode ser reduzido
- Exemplo: ciphertext-only criptanálise do DES
  - blocos compostos de oito bits ASCII, cada um com bit de paridade
  - Probabilidade de uma decriptação de *t* mensagens cifradas "acertar" **todos** os *t* bits de integridade nas mensagens planas é 2^{-t}
  - Podemos usar essa informação de paridade para filtrar chaves incorretas

Triple DES

- Necessidade de substituição do DES
  - Diversos ataques demonstrados
  - Ataques de busca exaustiva de chave
- Possibilidade: usar múltiplas repetições do DES
- Double DES permite ataque "meet-in-the-middle"
- Três encriptações oferecem bem mais segurança

Triple DES

- Variação do DES – tripla encriptação com duas ou três chaves
- Padrão estabelecido em ANSI X9.17 & ISO 8732
- Ataques práticos ainda desconhecidos
  - Força-bruta bastante inviável
  - Ataque meet-in-the-middle com três chaves precisa de 2^{112} operações e 2^{56} memória
- Alternativa ainda popular

Dupla e tripla encriptações

- Dupla encriptação: $E(x) = E_{K_2}(E_{K_1}(x))$
- Tripla encriptação: $E(x) = E'_{K_3}(E'_{K_2}(E'_{K_1}(x)))$
  - E'_K pode denotar E_K ou $D_K = E_K^{-1}$
  - O caso $E(x) = E_{K_3}(D_{K_2}(E_{K_1}(x)))$ é denominado E-D-E tripla encriptação
    - O subcaso $K_1 = K_3$ é denominado tripla encriptação de duas chaves

Triple DES (cont.)

- Duas chaves
  - Seqüência E-D-E
  - $E(x)=E_{K_1}(D_{K_2}(E_{K_1}(x)))$
  - Padronizado em ANSI X9.17 e ISO8732
  - Sem ataques práticos conhecidos
- Três chaves
  - $E(x)=E_{K_3}(D_{K_2}(E_{K_1}(x)))$
  - Oferece maior segurança
  - Adotado por algumas aplicações Internet, como PGP e S/MIME

AES – Advanced Encryption Standard

- Uma substituição do DES mostrava-se necessária
  - Diversos ataques teóricos demonstrados
  - Diversos ataques de busca exaustiva de chave
- Triple-DES podia ser usado – mas era lento
- NIST efetuou uma "chamada de cifras" em 1997
- 15 candidatos aceitos em Junho de 1998
- 5 selecionados para fase seguinte em Agosto de 1999
- Rijndael selecionado como AES em Outubro de 2000
- Publicado como padrão FIPS PUB 197 em Novembro de 2001

Requisitos do AES

- Cifra de chave simétrica
- Blocos de 128 bits, chaves de 128/192/256 bits
- Mais rápido e forte que Triple-DES
- Vida útil de 20 a 30 anos
- Especificações completas e detalhes de projeto
- Implementações em Java e C

Critérios de avaliação AES

- Critério inicial:
  - segurança – esforço para criptanalisar
  - custo – computacional
  - Algoritmo e características de implementação
- Critério final:
  - Segurança geral
  - Facilidade de implementação (software e hardware)
  - flexibilidade

O selecionados do AES

- Lista de Agosto de 1999:
  - MARS (IBM) - complexo, rápido, alta margem de segurança
  - RC6 (EUA) - muito simples, muito rápido, pequena margem de segurança
  - Rijndael (Bélgica) - limpo, rápido, boa margem de segurança
  - Serpent (Europa) – limpo, lento, altíssima margem de segurança
  - Twofish (EUA) - complexo, muito rápido, alta margem de segurança

O selecionados do AES

- Análises posteriores revelaram as diferenças-chave entre os selecionados
  - Estratégia de rounds
    - Poucos rounds complexos versus muitos rounds simples
  - Inovação
    - Redefinições de cifras existentes versus novas propostas

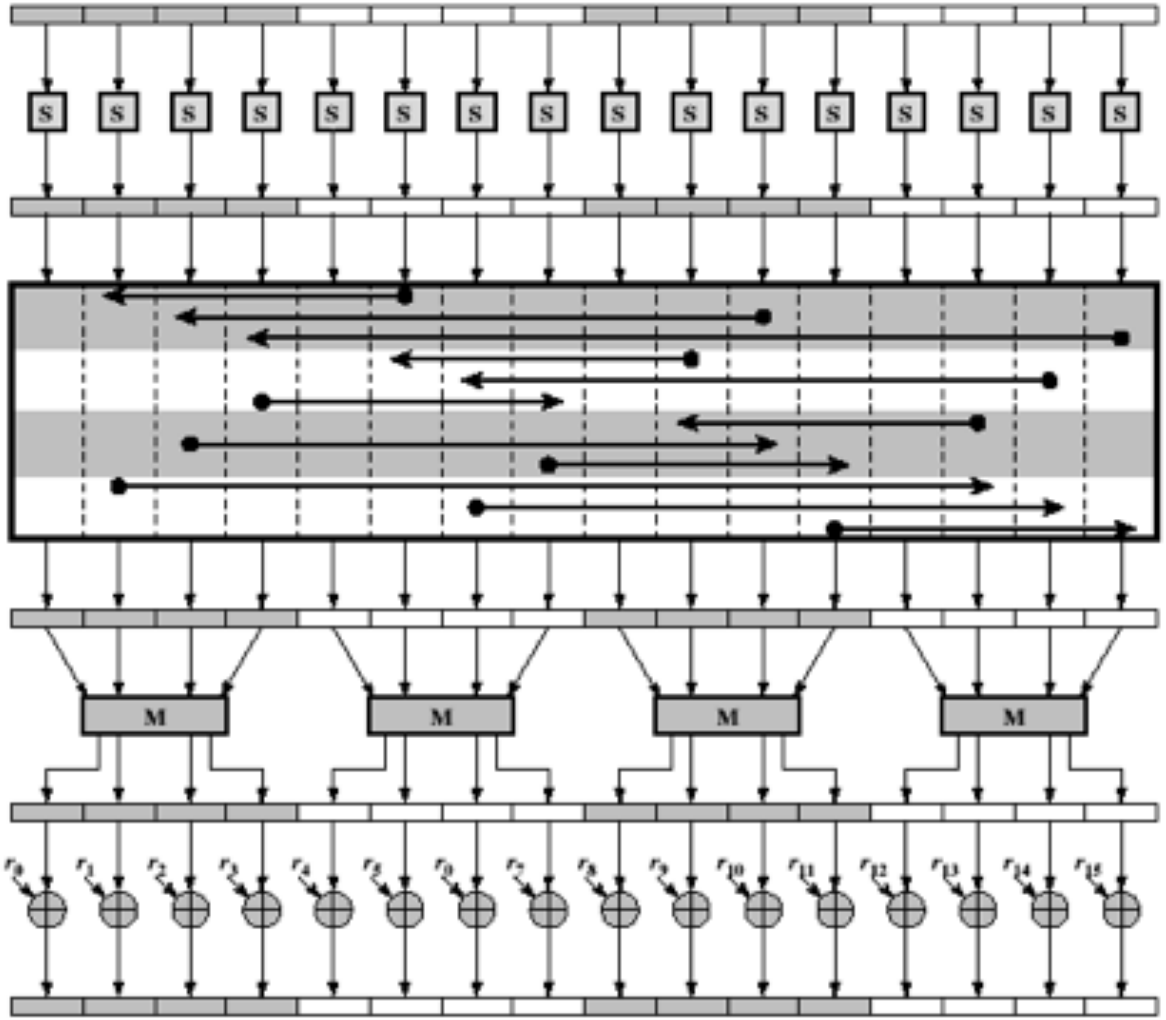
O AES – Rijndael

- Projetado por Rijmen-Daemen na Belgica
- Cifra iterativa, em vez de Feistel
  - Manipula dado em 4 grupos de 4 bytes
  - Opera o bloco inteiro em cada round
- Objetivos de projeto
  - Resistencia contra ataques conhecidos
  - Velocidade e código compacto em diversas CPUs
  - Projeto simples

Rijndael

- Processa blocos em quatro grupos de 4 bytes
- possui 9/11/13 rounds nos quais executa:
  - Substituição de bytes (um S-box para todos os bytes)
  - Deslocamento de linhas
  - Mistura de colunas
  - Adição (XOR) da subchave do round
- Possui um XOR inicial e o último round é incompleto
- Todas as operações podem ser combinadas em operações XOR e buscas em tabela
  - Bastante rápido e eficiente

Round AES



Aspectos de implementação

- Implementação eficiente em CPU 8 bits
  - Substituição de bytes usando tabela com 256 entradas
  - Deslocamento de linha é deslocamento de byte
  - Adição de chave é byte XOR
  - Mistura de colunas pode ser simplificada com busca em coluna

Aspectos de Implementação

- Implementação eficiente em CPU 32 bits
  - Redefina passos para usar palavras de 32 bits
  - precompute 4 tabelas de 256 palavras
  - Cada coluna em cada round pode ser precomputada usando 4 buscas em tabela + 4 operações XOR
  - Custo de 16Kb para armazenar tabelas
- Projetistas crêem que esta implementação eficiente foi decisiva na escolha do Rijndael