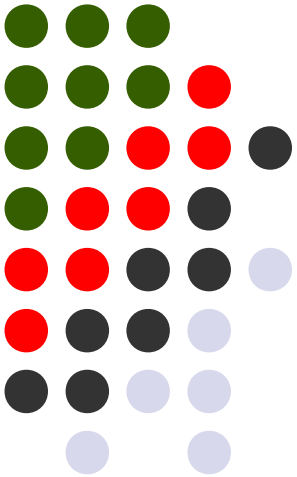
TES16– Introdução à Segurança da Informação
Módulo 05: Criptografia Básica

Prof. Charles Christian Miers
e-mail: charles.miers@udesc.br



UDESC

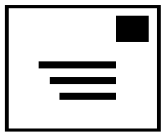
Segurança (Cont.)

- “A matemática é perfeita; a realidade é subjetiva. A matemática é definida; os computadores são teimosos. A matemática é lógica; as pessoas são irregulares, caprichosas e pouco compreensíveis.” Schneier, pg. 11

- “Segurança não é um produto; em si, ela é um processo.” Schneier, pg. 12

Elementos da Comunicação

Emissor
Remetente
BOB



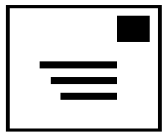
Mensagem

Meio

Receptor
Destinatário
ALICE

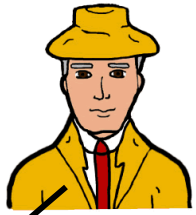
Problemas da Comunicação

BOB



Mensagem

Oponente

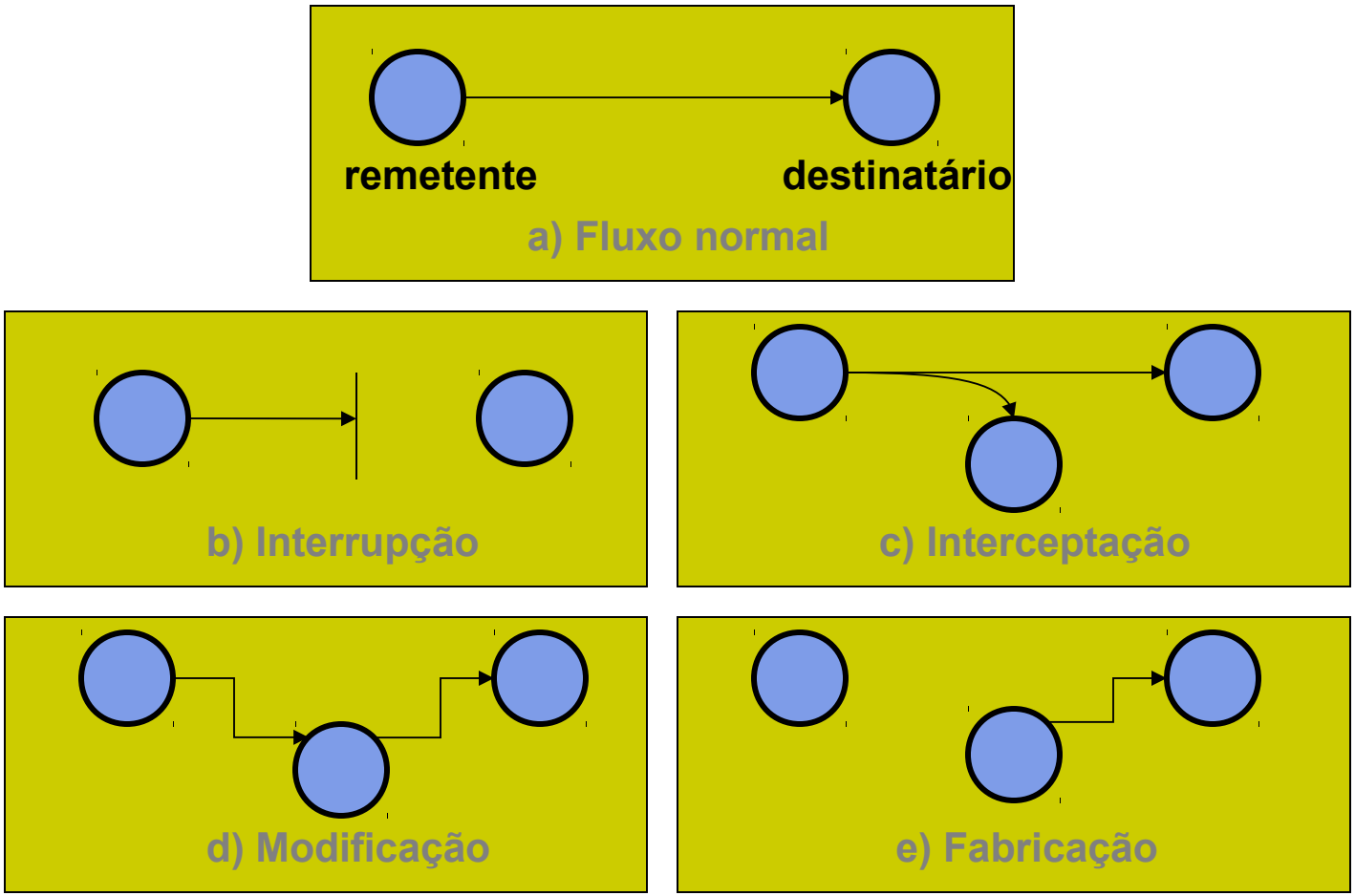


ALICE

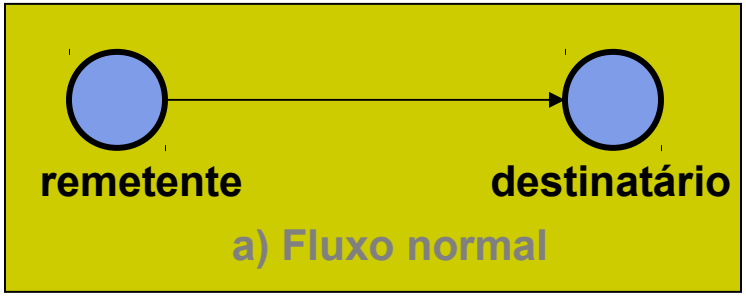
A mensagem pode passar pelo meio e ser violada, conhecida, alterada ou até mesmo criada por outros

Meio

Ataques em Comunicação



Ataques x Requisitos



INTERRUPÇÃO X DISPONIBILIDADE	INTERCEPTAÇÃO X CONFIDENCIALIDADE
MODIFICAÇÃO X INTEGRIDADE	FABRICAÇÃO X AUTENTICIDADE

Como implementar a segurança ?

- Usar criptografia para embaralhar dados transmitidos através de meios inseguros
- Definir um protocolo criptográfico para a troca segura de dados

Legislação

"... É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal"

Constituição Federal do Brasil, Art. 5º $ Xii

Criptografia

- Kriptos = oculto
- Objetivo: Não é ocultar a existência da mensagem e sim seu conteúdo ou significado
- Dois processos básicos:
  - Cifrar
  - Decifrar

Criptografia: Terminologia Básica

- **Texto original** – mensagem original
- **Cifra de texto** - mensagem codificada
- **Cifra** - algoritmo que transforma o texto original para texto cifrado
- **Chave** - informação usada na cifra conhecida somente ao emissor/receptor
- **Cifrar** – converte o texto original para o texto cifrado
- **Decifrar** - recupera o texto cifrado para texto original
- **Criptografia** – estuda a cifragem princípios/métodos
- **Criptoanálise (quebra de código)** – estuda os princípios/métodos de decifragem do texto cifrado *sem* saber a chave
- **Criptologia** – campo da criptografia e da criptoanálise

Criptografia: Classificação

- O sistema criptográfico pode ser classificado por:
  - Tipos de operações de cifragem usadas
    - Substituição / Transposição / Produto
  - Número de chaves usadas
    - Chave única ou privada / duas chaves ou pública
  - Maneira em que o texto original é processado
    - Bloco/ caractere (cadeia)

Cifras Clássicas de Substituição

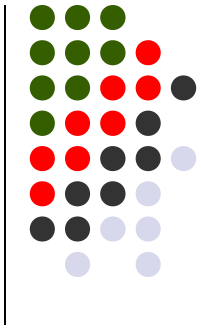
- Letras do texto original são substituídas por outras letras, por números e/ou por símbolos
- O texto original pode ser visto como uma sequência de bits, e então, a substituição envolve a substituição de padrões de bits do texto original por padrões de bits do texto cifrado

Criptografia: Método de Substituição

- Método de substituição:
  - Consiste em uma representação ao acaso de uma letra por outra. Usa-se o alfabeto com seus pares de letras para cifrar e decifrar mensagens

A	D	H	I	K	M	O	R	S	U	W	Y	Z
V	X	B	G	J	C	Q	L	N	E	F	P	T

- Assim:
  - Para a mensagem **seguranca em computacao**, teríamos o texto cifrado **NUIELVSMV UC MQCIEZVMVQ**.



Criptografia: Método de Substituição

- Método de substituição
  - Exemplo: Cifra de César (deslocamento)
    - Deslocamento de 3 casas para cada letra do alfabeto

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
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

- Para a mensagem **segurança em computação**, é gerado o texto cifrado: **VHJXUDQFD HP FRPSXWDFDR**

Criptoanálise: Origem Histórica

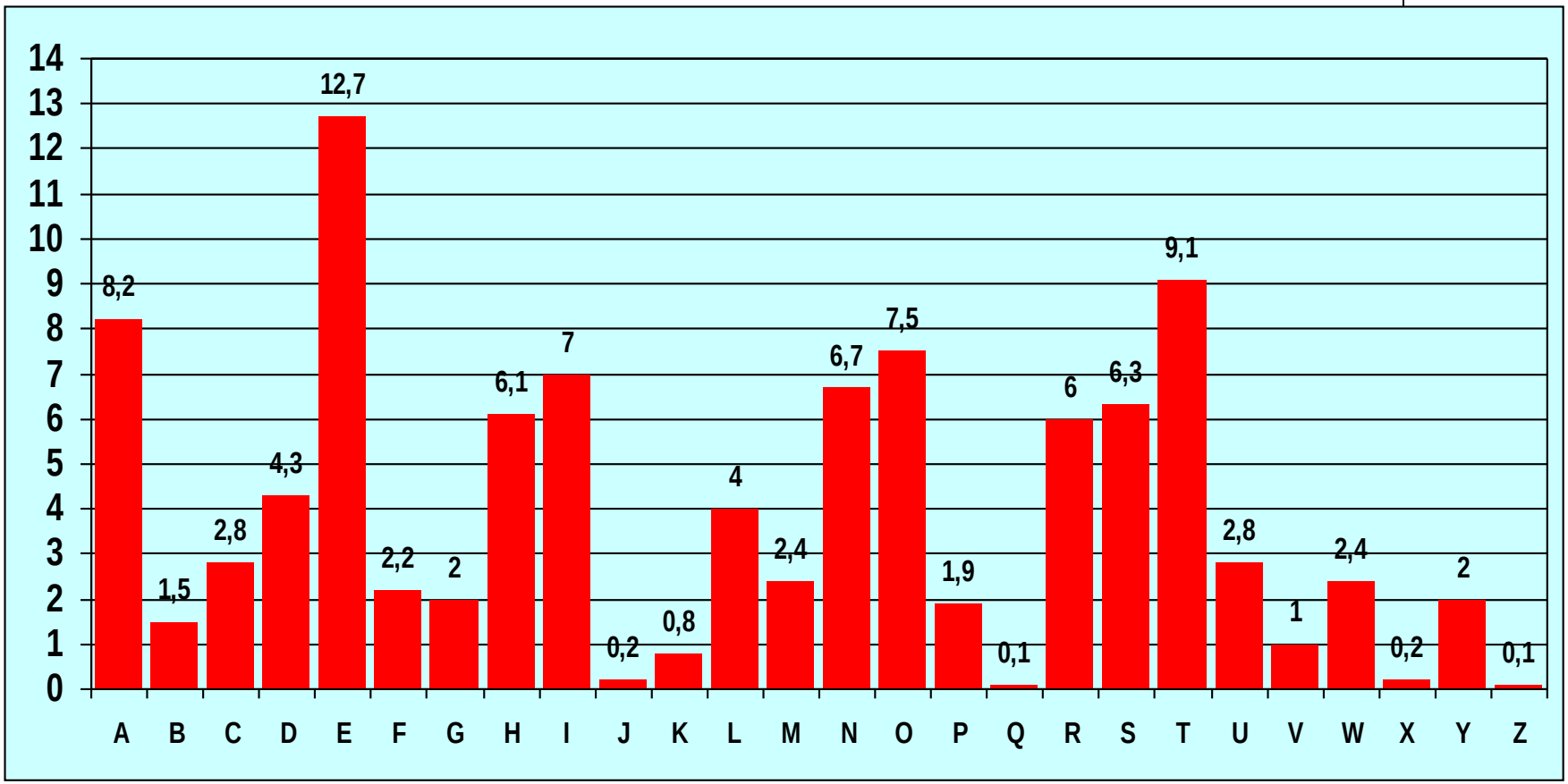
- Os Árabes:
  - Empregavam cifras e estudavam a quebra dos segredos sem o uso da chave
  - Inventaram a criptoanálise
  - Avanços dos estudos da matemática, estatística e linguística
- Criptoanálise: Ciência que permite a descoberta de uma mensagem sem o conhecimento da chave utilizada para ocultá-la
- O estudo da frequência das letras revelou que algumas aparecem mais que outras em um texto:
  - No idioma árabe, as letras A e L aparecem mais. A letra J aparece dez vezes menos

Criptoanálise:Força Bruta

- Método sempre possível de ser aplicado, consiste em simplesmente cada uma das possíveis chaves até encontrar a chave empregada
- O ataque mais básico, proporcional ao tamanho chave
- Supor que qualquer um saiba/reconhece o texto original

Tamanho da Chave (bits)	Número de Chaves alternativas	Tempo requerido para uma decifragem/µs	Tempo requeridp para 10^6 decigrafens/µs
32	$2^{32} = 4.3 \times 10^9$	2^{31} µs = 35.8 minutos	2.15 milisegundos
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} µs = 1142 anos	10.01 horas
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} µs = 5.4×10^{24} anos	5.4×10^{18} anos
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} µs = 5.9×10^{36} anos	5.9×10^{30} anos
26 caracteres (permutação)	$26! = 4 \times 10^{26}$	2×10^{26} µs= 6.4×10^{12} anos	6.4×10^6 anos

A Frequência no inglês



Baseada em passagens extraídas de jornais e romances. Amostragem total de 100.362 caracteres. Simon Singh, pg. 36

A Análise de frequência

- É uma ferramenta da criptoanálise
- Exige astúcia e raciocínio lógico
- Uma tentativa de decifrar um texto através dela, pode ser frustrada pela simples troca da letra mais frequente do alfabeto
- As letras mais frequentes do texto cifrado podem estar em ordem trocada com as letras mais frequentes do alfabeto

Criptoanalisando um texto cifrado

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CY SX'XJMY, KBO JCKO XPV EYKKOV LBO DJCMPV ZOYCJO BYS, KXUYPD: "DJOXL EYPD, YCJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO YXZROK CY FXKL XDOK XPV LBO RODOPVK CY XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X YXNCMJ CY UCMJ SXGOKLU?"

OFYRCDMO, LXROK YJCS LBO LBCMKXPV XPV CPO PYDBLK

Criptoanalisando um texto cifrado

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CY SX'XJMY, KBO JCKO XPV EYKKOV LBO DJCMPV ZOYCJO BYS, KXUYPD: "DJOXL EYPD, YCJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO YXZROK CY FXKL XDOK XPV LBO RODOPVK CY XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X YXNCMJ CY UCMJ SXGOKLU?"

OFYRCDMO, LXROK YJCS LBO LBCMKXPV XPV CPO PYDBLK

a) O texto é curto e a aplicação da análise de frequência seria muito simples e ingênuo;

b) Voltar a atenção para as três letras que mais ocorrem:

O = 38 vezes, X = 34 vezes e o P = 31 vezes

Será que O = e, X = t e P = a?

Criptoanalisando um texto cifrado

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CY SX'XJMY, KBO JCKO XPV EYKKOV LBO DJCMPV ZOYCJO BYS, KXUYPD: "DJOXL EYPD, YCJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO YXZROK CY FXKL XDOK XPV LBO RODOPVK CY XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X YXNCMJ CY UCMJ SXGOKLU?"

OFYRCDMO, LXROK YJCS LBO LBCMKXPV XPV CPO PYDBLK

Será que O = e, X = t e P = a?

A e X são vogais pois são mais amigáveis com as demais letras dos que P

A e E são as vogais mais populares no inglês

O = e ? ou O = a ?

X = a ? ou X = e ?

	A	B	C	D	E	F	G	H	I	J														Z
O	1	9	0	3	1	1	1	0	1	4														2
X	0	7	0	1	1	1	1	0	2	4														1
P	1	0	5	6	0	0	0	0	0	1	1	2	2	0	8	0	0	0	0	0	0	11	0	9	9	0

Criptoanalisando um texto cifrado

PCQ VMJYPD LBYK LYSe KBaBJaWaV BaV ZCJPe EYPD KBaBJYUaJ LBJee KCPK. CP LBe LBCMKaPV aPV IYJKL PYDBL, QBeP KBe BaV ePVeV LBe LaRe CY Sa'aJMY, KBe JCKe aPV EYKKeV LBe DJCMPV ZeYCJe BYS, KaUYPD: "DJeaL EYPD, YCJ a LBCMKaPV aPV CPe PYDBLK Y BaNe ZeeP JeACMPLYPD LC UCM LBe YaZReK CY FaKL aDeK aPV LBe ReDePVK CY aPAYePL EYPDK. SaU Y SaEe KC ZCRV aK LC AJaNe a YaNCMJ CY UCMJ SaGeKLU?"

eFYRCDMe, LaReK YJCS LBe LBCMKaPV aPV CPe PYDBLK

O = e - pois aparece OO

X = a - pois aparece sozinho

Criptoanalisando um texto cifrado

PCQ VMJiPD LBiK LiSe KBaBJaWaV BaV ZCJPe EiPD KBaBJiUaJ LBJee KCPK. CP LBe LBCMKaPV aPV IiJKL PiDBL, QBeP KBe BaV ePVeV LBe LaRe Ci Sa'aJMi, KBe JCKe aPV EiKKeV LBe DJCMPV ZeiCJe BiS, KaUiPD: "DJeaL EiPD, iCJ a LBCMKaPV aPV CPe PiDBLK i BaNe ZeeP JeACMPLiPD LC UCM LBe iaZReK Ci FaKL aDeK aPV LBe ReDePVK Ci aPAiePL EiPDK. SaU i SaEe KC ZCRV aK LC AJaNe a iaNCMJ Ci UCMJ SaGeKLU?"

eFiRCDMe, LaReK iJCS LBe LBCMKaPV aPV CPe PiDBLK

O = e - pois aparece OO

X = a - pois aparece sozinho

Y = i - palavra inteira só com uma letra

Criptoanalisando um texto cifrado

PCQ VMJiPD LhiK LiSe KhahJaWaV haV ZCJPe EiPD KhahJiUaJ LhJee KCPK. CP Lhe LhCMKaPV aPV liJKL PiDhL, QheP Khe haV ePVeV Lhe LaRe Ci Sa'aJMi, Khe JCKe aPV EiKKeV Lhe DJCMPV ZeiCJe hiS, KaUiPD: "DJeaL EiPD, iCJ a LhCMKaPV aPV CPe PiDhLK i haNe ZeeP JeACMPLiPD LC UCM Lhe iaZReK Ci FaKL aDeK aPV Lhe ReDePVK Ci aPAiePL EiPDK. SaU i SaEe KC ZCRV aK LC AJaNe a iaNCMJ Ci UCMJ SaGeKLU?"

eFiRCDMe, LaReK iJCS Lhe LhCMKaPV aPV CPe PiDhLK

O = e - pois aparece OO

X = a - pois aparece sozinho

Y = i - palavra inteira só com uma letra

B = h - aparece com frequência na frente de e

Criptoanalisando um texto cifrado

As palavras mais comuns no Inglês são THE e AND.

No texto cifrado existe:

Lhe - aparece seis vezes

aPV - aparece cinco vezes

Logo: L representa t, P representa n e V provavelmente representa d

nCQ dMJinD thiK tiSe KhahJaWad had ZCJne EinD KhahJiUaJ thJee KCnK. Cn the thCMKand and IiJKt niDht, Qhen Khe had ended the taRe Ci Sa'aJMi, Khe JCKe and EiKKed the DJCMnd ZeiCJe hiS, KaUinD: "DJeat EinD, iCJ a thCMKand and Cne niDhtK i haNe Zeen JeACMntinD tC UCM the iaZReK Ci FaKt aDeK and the ReDendK Ci anAient EinDK. SaU i SaEe KC ZCRd aK tC AJaNe a iaNCMJ Ci UCMJ SaGeKtU?"

eFiRCDMe, taReK iJCS the thCMKand and Cne niDhtK

Criptoanalisando um texto cifrado

A segunda frase começa com Cn. C provavelmente é uma vogal.

X = a, O = e, Y = i, C = o, pois não poderia ser u.

noQ dMJinD thiK tiSe KhahJaWad had ZoJne EinD KhahJiUaJ thJee KonK. on the thoMKand and IiJKt niDht, Qhen Khe had ended the taRe oi Sa'aJMi, Khe JoKe and EiKKed the DJoMnd ZeioJe hiS, KaUinD: "DJeat EinD, ioJ a thoMKand and one niDhtK i haNe Zeen JeAoMntinD to UoM the iaZReK oi FaKt aDeK and the ReDendK oi anAient EinDK. SaU i SaEe Ko ZoRd aK to AJaNe a iaNoMJ oi UoMJ SaGeKtU?"

eFiRoDMe, taReK iJoS the thoMKand and one niDhtK

Criptoanalisando um texto cifrado

Temos ainda a ocorrência de Khe.

K pode ser t ou s, mas t foi representado por L. Logo K = s.

noQ dMJinD this tiSe shahJaWad had ZoJne EinD shahJiUaJ thJee sons. on the thoMsand and IiJst niDht, Qhen she had ended the taRe oi Sa'aJMi, she Jose and Eissed the DJoMnd ZeioJe hiS, saUinD: "DJeat EinD, ioJ a thoMsand and one niDhts i haNe Zeen JeAoMntinD to UoM the iaZRes oi Fast aDes and the ReDends oi anAient EinDs. SaU i SaEe so ZoRd as to AJaNe a iaNoMJ oi UoMJ SaGestU?"

eFiRoDMe, taRes iJoS the **thoMsand and one niDhts**

O texto decifrado

Now during this time shahrazad had borne king shahriyar three sons. On the thousand and first night, when she had ended the tale of ma'aruf, she rose and kissed the ground before him, saying: "great king, for a thousand and one nights i have been recounting to you the fables of past ages and the legends of ancient kings. May i make so bold as to crave a favour of your majesty?"

Epilogue, tales from the thousand and one nights

Criptografia: Método de Transposição

- Conhecida também como transposição clássica ou cifras de permutação
- Esconde-se a mensagem (texto original) rearranjando a ordem dos caracteres
- Não são alterados os caracteres originais usados
- A decifragem ocorre caso se tenha a mesma distribuição de frequência como o texto original

Criptografia: Método de Transposição

- Método de transposição:
  - Troca a ordem das letras da mensagem utilizando um determinado critério e gerando um anagrama
  - Uma palavra de três letras pode gerar apenas seis combinações diferentes:
    - Exemplo: PAI -> PIA -> AIP -> API -> IAP -> IPA
  - Transposição ao acaso eleva a segurança, entretanto, aumenta as dificuldades de recuperação da mensagem

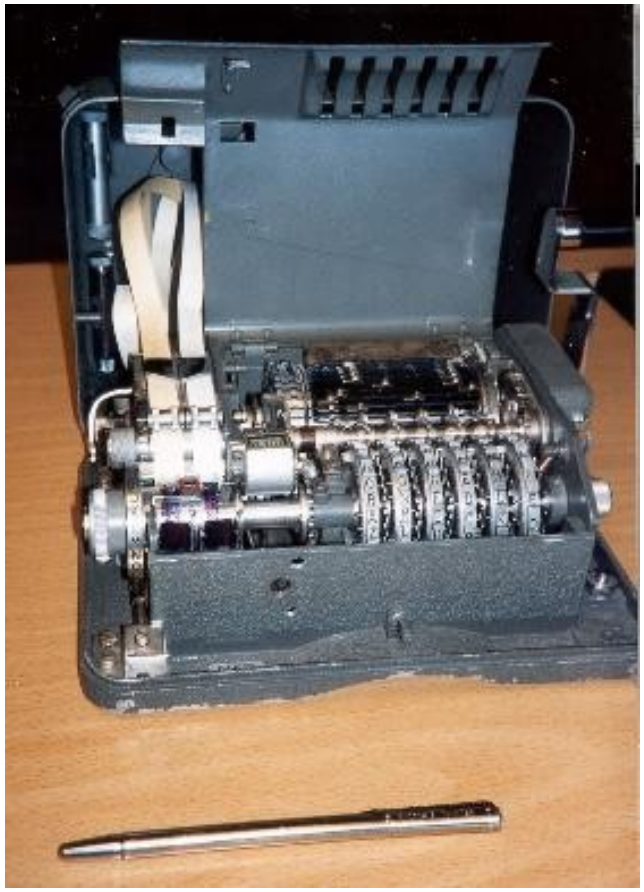
Criptografia: Método do Produto

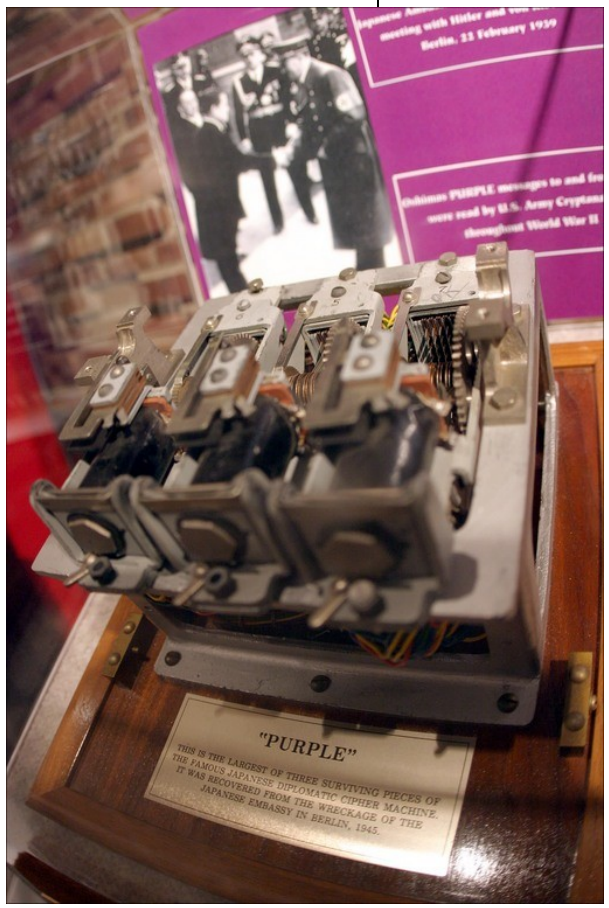
- Cifras usando substituição ou transposição não são seguras por causa das características da linguagem
- Deve-se considerar usar várias cifras sucessivamente para tornar o método mais resistente/robusto, então:
  - Duas substituições fazem uma substituição mais complexa
  - Duas transposições fazem uma transposição mais complexa
  - Uma substituição seguida por uma transposição faz uma nova cifra muito mais forte
- Considerado o elo entre as cifras clássicas e as modernas

Criptografia: Máquinas de Rotor

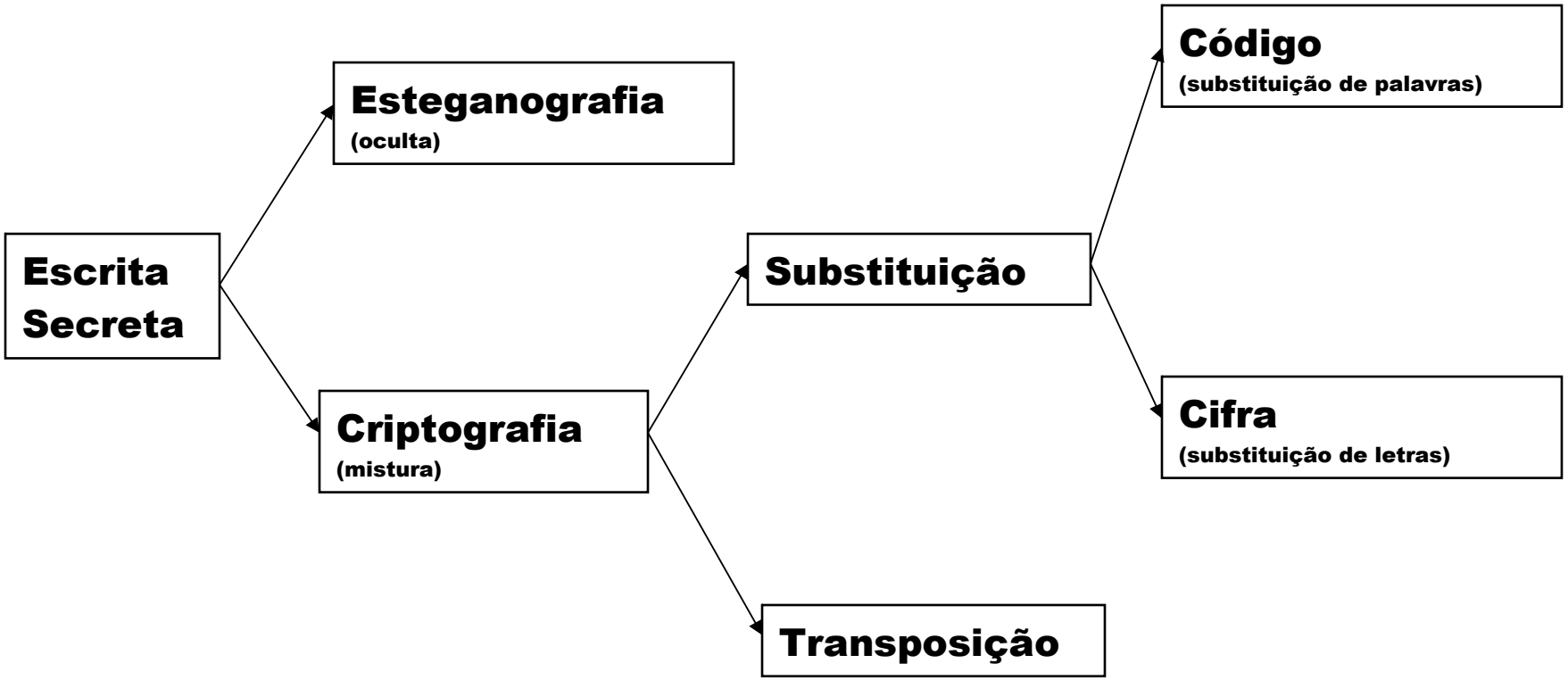
- Antes das cifras modernas,as máquinas rotor eram as cifras complexas mais comuns em uso
- Extensamente usado na 2ª Guerra Mundial
  - Alemanha: Enigma
  - Aliados Hagelin
  - Japão: Púrpura (*Purple*)
- Executam cifras muito complexas, variando a substituição
- Empregam uma série de cilindros, cada um dando substituição, o qual gira e muda depois que cada letra foi cifrada
- Com três cilindros possui 26^3=17576 alfabetos

Criptografia: Máquinas de Rotor





Escrita Secreta: Classificação



Esteganografia

- Esconde a existência da mensagem em outros elementos
  - Pode usar um subconjunto de letras/palavras em uma mensagem mais longa, marcada de algum modo
  - Usando a tinta invisível
  - Esconder a mensagem sobrescrevendo o LSB (*Less Significative Bits*) em arquivos de som, imagem e vídeo
- Inconvenientes
  - Despesas gerais elevadas para esconder relativamente poucos bits de informação (*payload*)

Esteganografia: Texto

Exemplo (mensagem escondida em um texto):

O Senhor Evandro quer usar este salão temporariamente.
Relembre o fato ocorrido, isto poderia estragar relíquias, florais e imagens talhadas. Obrigado.

O Senhor **E**vandro **q**uer **u**sar **e**ste **s**alão **t**emporariamente.
Relembre **o** **f**ato **o**corrido, **i**sto **p**oderia **e**stragar relíquias, **f**lorais **e** **i**magens **t**alhadas. **O**brigado.

O sequestro foi perfeito

Esteganografia: Imagens

- A figura 1 é a imagem original
- A figura 2 possui cinco livros de Shakespeare incorporados nos LSB através de um software de esteganografia

Fig. 1: Zebras

Fig. 2: Hamlet, Macbeth, Julius Caesar Merchant of Venice, King Lear

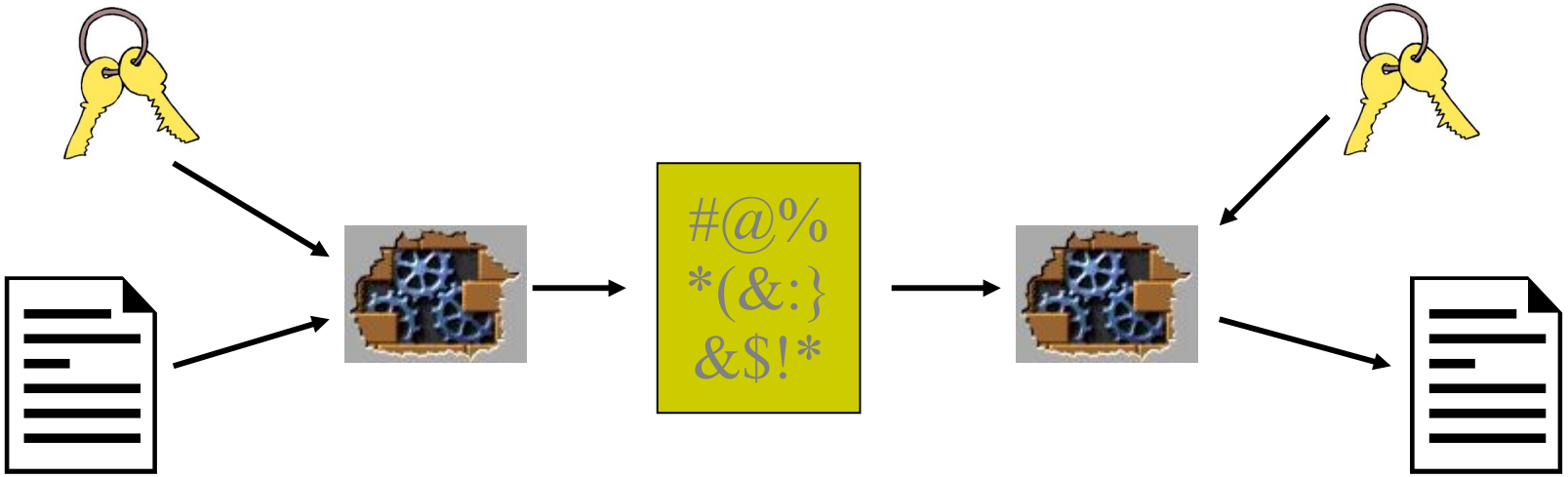
Criptografia Moderna

- Diferentemente da esteganografia possui uma relação 1:1 entre texto original e texto cifrado, quer seja em caractere (cifra) ou palavras (código)
- Diversos métodos podem ser empregados para embaralhar os dados
- Criptografia Moderna dividida em duas classes principais:
  - Cifradores Simétricos, também conhecido como de chave secreta/compartilhada
  - Cifradores Assimétricos, também conhecido como de chave pública
- As classificações diferem, em essência, no modo de manipulação da(s) chave(s)
- Usada comumente para implementar protocolos de comunicação criptográficos

Criptografia Simétrica

ALICE

BOB

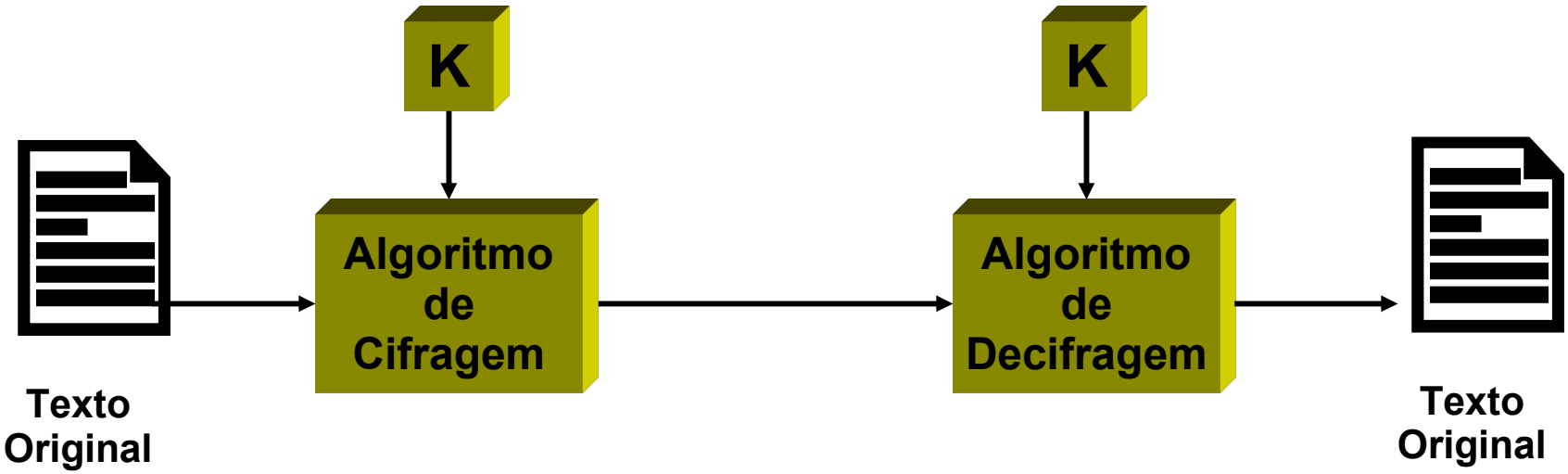


Elementos da Comunicação

ALICE

A troca da chave entre Alice e Bob deve ser segura.
Ele deve também ser combinada antes.

BOB



Considerações: Segundo Stallings

Sistemas criptográficos são genericamente classificados em três dimensões

- Tipos de operações utilizadas na cifragem:
  - Uso dos princípios de substituição e transposição em diversos estágios
  - É importante que o processo possa ser revertido sem perdas de informações
- Número de chaves utilizadas:
  - Quando o emissor e o receptor utilizam a mesma chave, o processo é conhecido com simétrico, de chave única, chave secreta ou cifragem convencional
- Forma com que o texto original é processado:
  - Um cifrador de blocos produz um bloco por vez para cada bloco do texto aberto
  - Um cifrador contínuo (*streaming*), processa continuamente o texto original gerando um único bloco (maior) de saída

Considerações: Segundo Schneier

Criptosistemas simétricos tem os seguintes problemas

- As chaves devem ser distribuídas em segredo
  - Como trocar chaves sem que as mesmas sejam comprometidas? Pessoalmente?
- Pode existir fabricação de mensagens
  - Se a chave for comprometida (descoberta) permitirá a leitura de todas as mensagens cifradas com essa chave. Poderá existir a fabricação de mensagens;
- Gerenciamento das chaves é trabalhoso
  - O número de chaves aumenta muito a medida que o número de usuários na rede aumenta. O gerenciamento das chaves é um problema:

Fórmula: n . (n - 1) /2 10 usuários = 10 . (10 - 1) / 2
10 usuários = 45 chaves cada um

Onde n é o número de usuários em uma rede

A Criptoanálise nesse Modelo

- Para conhecer o texto original, o receptor precisa saber a chave utilizada para cifrar e também o algoritmo
- A criptoanálise consiste na descoberta do texto original sem necessariamente conhecer a chave ou o algoritmo utilizados
- Quanto mais informações o criptoanalista possuir a respeito da mensagem cifrada, mais fácil será a análise e descoberta do segredo
- Deseja-se que no máximo, o criptoanalista conheça apenas o algoritmo criptográfico utilizado

Tipos de Ataques em Mensagens Cifradas

Tipo de ataque	Conhecimento do Criptoanalista
Somente texto cifrado	Algoritmo de criptografia Texto cifrado
Texto original conhecido	Algoritmo de criptografia Texto cifrado Um ou mais pares de texto original/cifrado
Texto original escolhido	Algoritmo de criptografia Texto cifrado Texto original escolhido para mostrar o comportamento do algoritmo
Texto cifrado escolhido	Algoritmo de criptografia Texto cifrado Texto cifrado escolhido para mostrar o comportamento do algoritmo
Texto escolhido	Algoritmo de criptografia Texto cifrado Texto original escolhido para mostrar o comportamento do algoritmo Texto cifrado escolhido para mostrar o comportamento do algoritmo

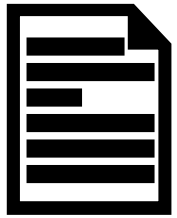
Protocolo Criptográfico

Criptografia Assimétrica

ALICE

Chaveiro de chaves públicas

BOB



Protocolo Criptográfico
Criptografia Assimétrica

1) Alice e Bob devem combinar o uso de um sistema criptográfico
2) Alice cifra o seu texto original com a chave pública de Bob utilizando o algoritmo criptográfico combinado. Gera o texto cifrado
3) Alice envia o texto cifrado para Bob
4) Bob decifra o texto cifrado com a sua chave privada utilizando o mesmo algoritmo que foi combinado com Alice

Notação das chaves

K - (***K****EY*) chave simétrica trocada entre as entidades para cifrar e decifrar as mensagens

KU - (*P**U**BLIC **K**EY*) chave pública de uma entidade que pode ser utilizada para cifrar e decifrar as mensagens

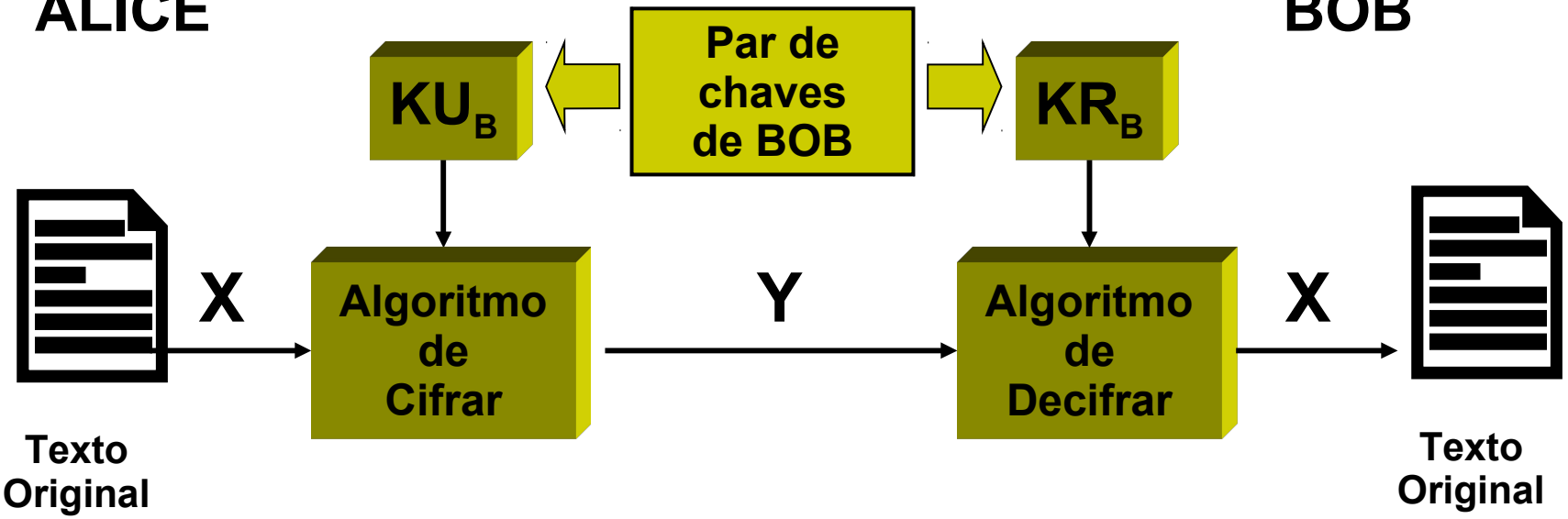
KR - (*P**R**IVATE **K**EY*) chave privada de uma entidade que pode ser utilizada para cifrar e decifrar as mensagens

Protocolo Criptográfico Assimétrico

ALICE

A chave pública de cada entidade pode ser utilzada para cifrar as mensagens.

BOB



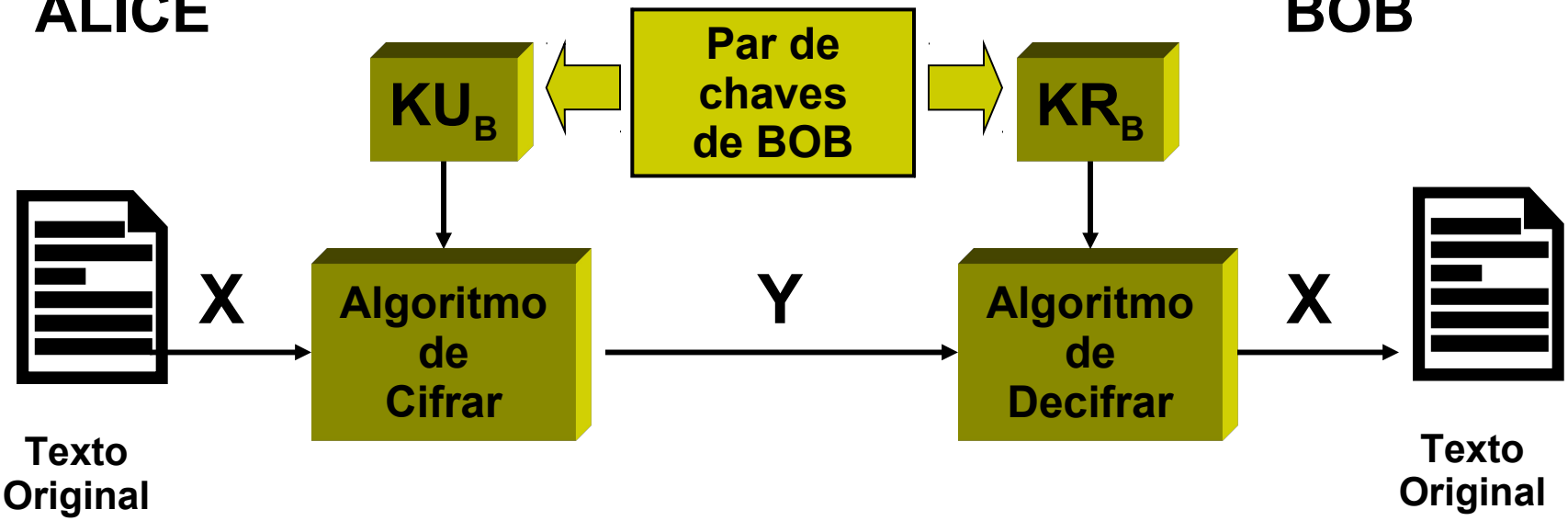
Comparativo: Simétrica x Assimétrica

Criptografia Convencional (Simétrica)	Criptografia Chave Pública (Assimétrica)
O mesmo algoritmo com a mesma chave devem ser utilizados para cifrar e decifrar	Um algoritmo é usado para cifrar e decifrar as mensagens, porém, um par de chaves é utilizado
O remetente e o destinatário devem compartilhar a chave e o algoritmo	O remetente e o destinatário devem ter a chave correspondente ao par da chave usada para cifrar ou decifrar a mensagem
A chave deve ser mantida em segredo	Uma das duas chaves deve ser mantida em segredo
Deve ser impossível ou impraticável se decifrar a mensagem sem outra informação adicional	Deve ser impossível ou impraticável se decifrar a mensagem sem outra informação adicional
O conhecimento do algoritmo e de exemplos de texto cifrado com ele, devem ser insuficientes para determinar a chave	O conhecimento do algoritmo e de exemplos de texto cifrado com ele, devem ser insuficientes para determinar a outra chave

Confidencialidade com Chave Pública

ALICE

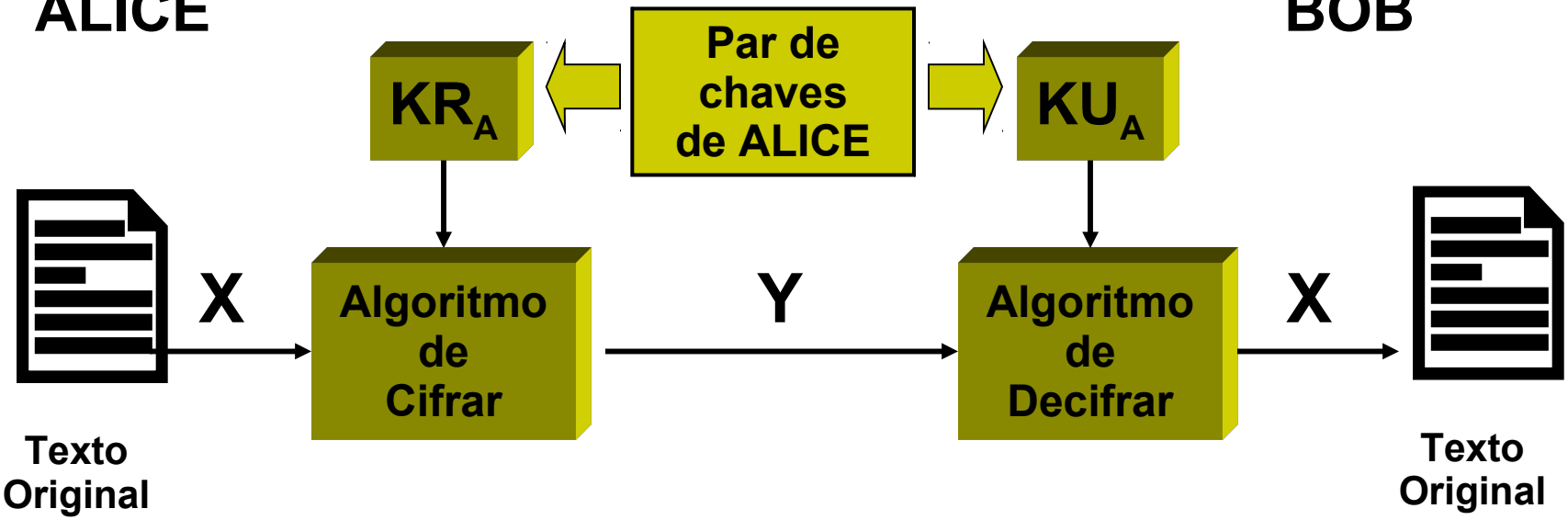
BOB



Autenticidade e Irretratabilidade com Chave pública

ALICE

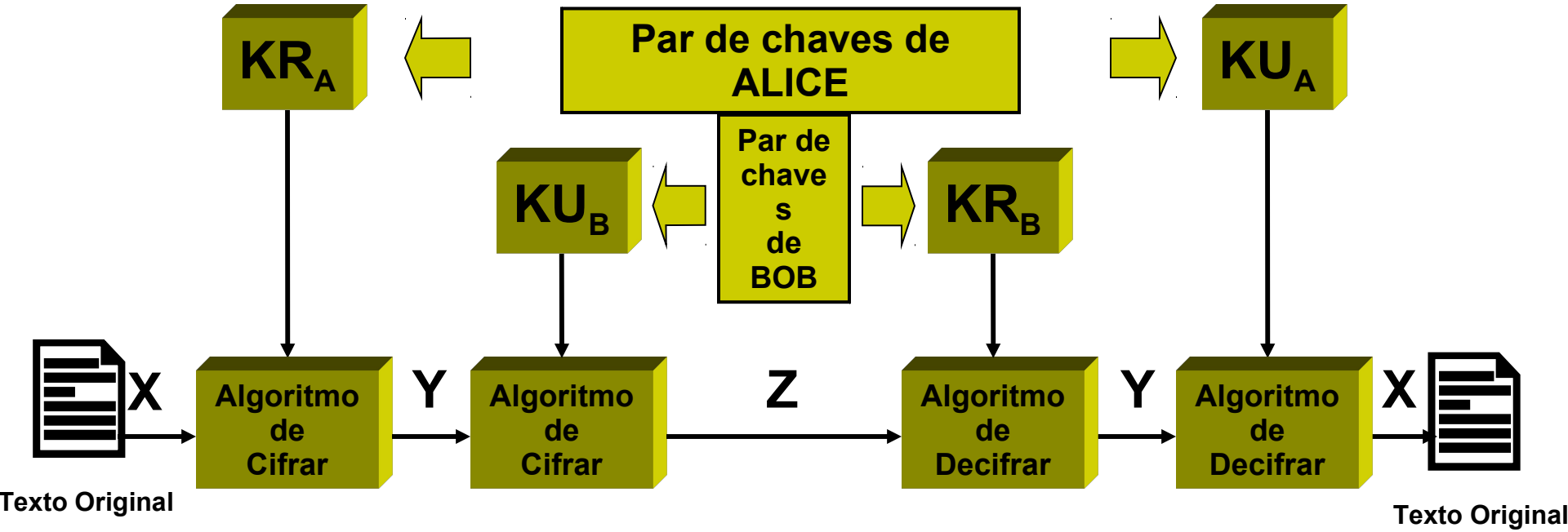
BOB



Autenticidade, Confidencialidade e Irretratabilidade com Chave Pública: Dupla Cifragem

ALICE

BOB



Entendendo a Notação

Z = Y cifrado com a chave pública de Bob
Y = Texto decifrado pela chave privada de Alice
X = Texto original

Cifrar: $Y = E_{KR_A}(X)$

$Z = E_{KU_B}(Y)$

Decifrar: $Y = D_{KR_B}(Z)$

$X = D_{KU_A}(Y)$

Cifrar: $Z = E_{KU_B}[E_{KR_A}(X)]$

Decifrar: $X = D_{KU_A}[D_{KR_B}(Z)]$

UDESC
Joinville

Departamento
de Ciência da
COMPUTAÇÃO

Leitura Recomendada: (Cont.)

- Stallings, Willian. *Network Security Essentials*. 2ª Edição. Editora Prentice-Hall. 2003.
  - Capítulos 1 e 2

- Stallings, William - *Cryptography and Network Security: Principles and Practice*. 4ª Edição. Prentice-Hall. 2006.
  - Capítulos 2, 3, 4, 5, 7, 9 e 10

- Terada, Routo - Segurança de Dados Criptografia em Redes de Computador. São Paulo. Edgard Blücher. 2000