Segurança em Redes de Computadores

Kelvin Lopes Dias

Diego dos Passos Silva
(kld/dps4@cin.ufpe.br)

Agenda

- Criptografia
  - Criptografia de Chave Simétrica
  - Criptografia de Chave Assimétrica
- Segurança de Redes
  - Confidencialidade e Integridade
  - Autenticação e Assinatura Digital
  - Gerenciamento de Chaves
- Segurança na Internet e Aplicações
  - IPSec e SSL/TLS
  - PGP, VPN e Firewalls

Visão Geral

- O que é segurança na rede?
  - Para uma mensagem ser segura, é necessário que apenas os envolvidos na mesma possam entender a mensagem. Para isso, ninguém mais pode **interceptar**, **ler** ou **executar** processos computacionais trocados entre os envolvidos.
  - Apenas o emissor e o receptor devem **entender** o conteúdo da mensagem.

Visão Geral

- Confidencialidade
- Autenticação
- Integridade
- Não-repudiação de mensagem
- Disponibilidade
- Controle de acesso

CRIPTOGRAFIA

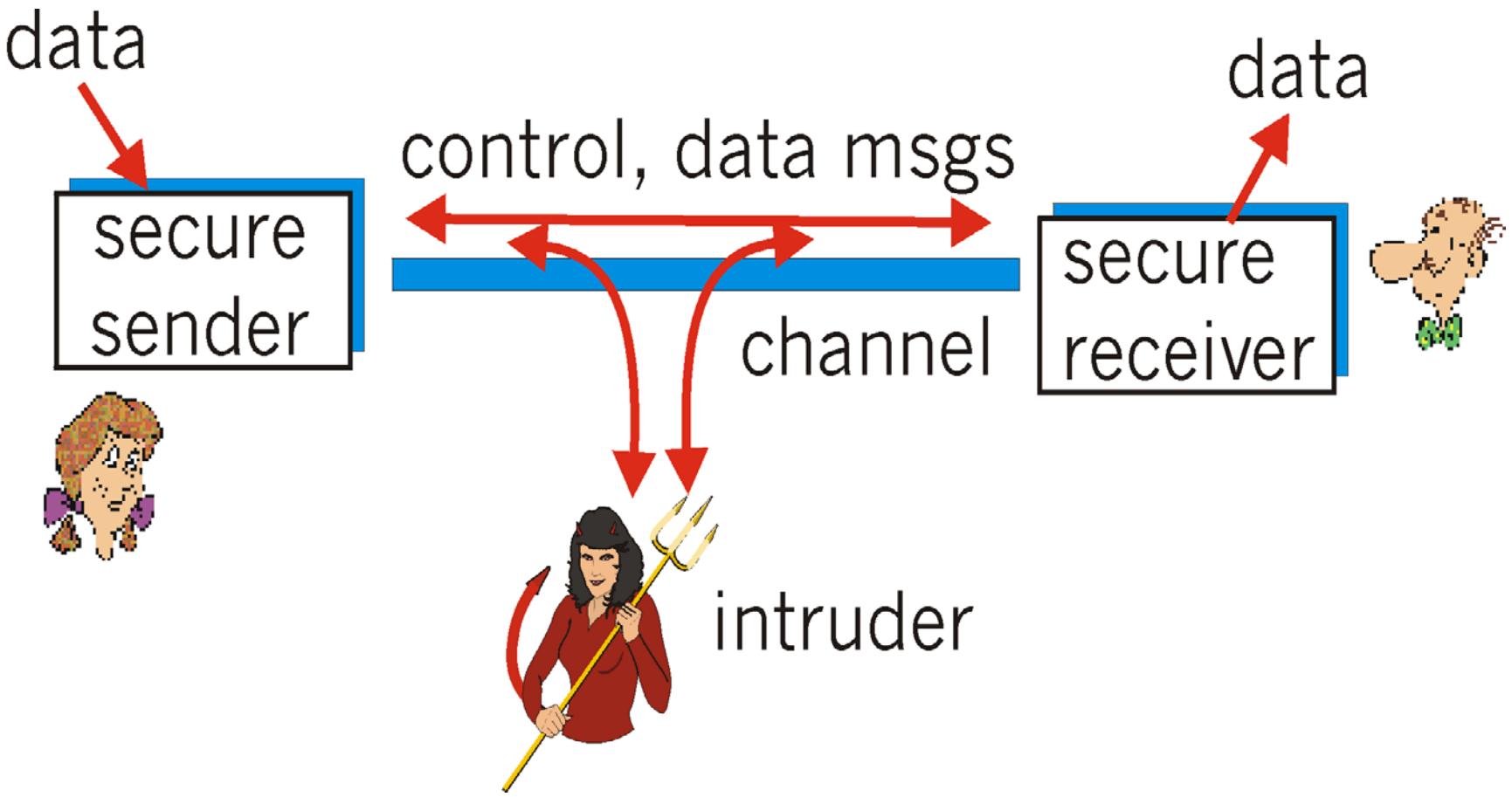
Introdução

- Do grego kriptós, “escondido” e gráphein, “escrita”.
- É uma das principais técnicas pelas quais a informação pode ser transformada de sua forma original para outra ilegível de forma que possa ser conhecida apenas pelo seu devido receptor.
- Ciência e a arte de transformar mensagens modo a torná-las seguras e imunes a ataques.

Introdução

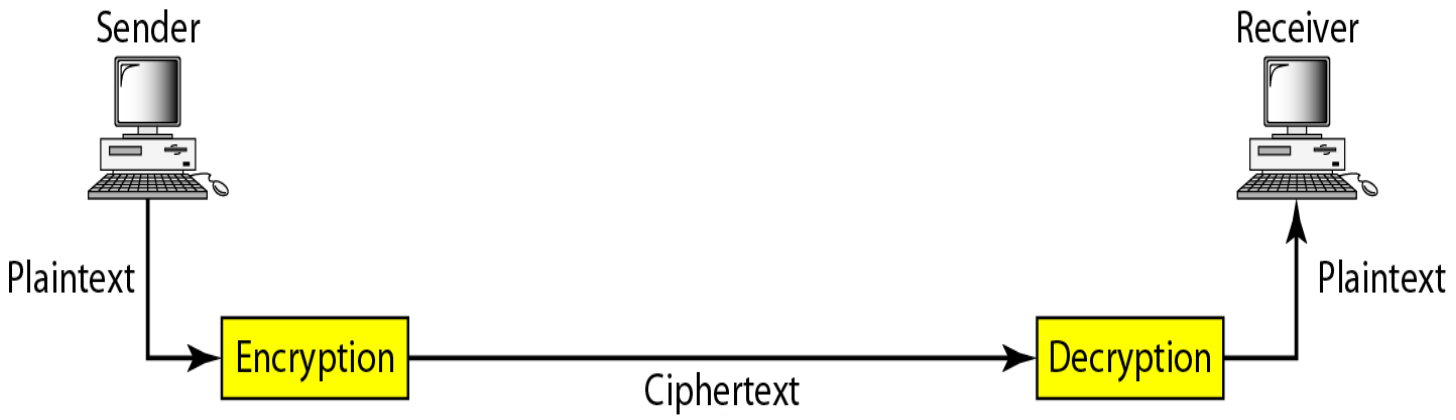
- A criptografia oferece confidencialidade, integridade, autenticação e o não repúdio de mensagens. Fornece também autenticação de entidades.
- Grande parte da segurança das redes modernas é alcançada através da criptografia.

Introdução


data
secure sender
control, data msgs
channel
data
secure receiver
intruder

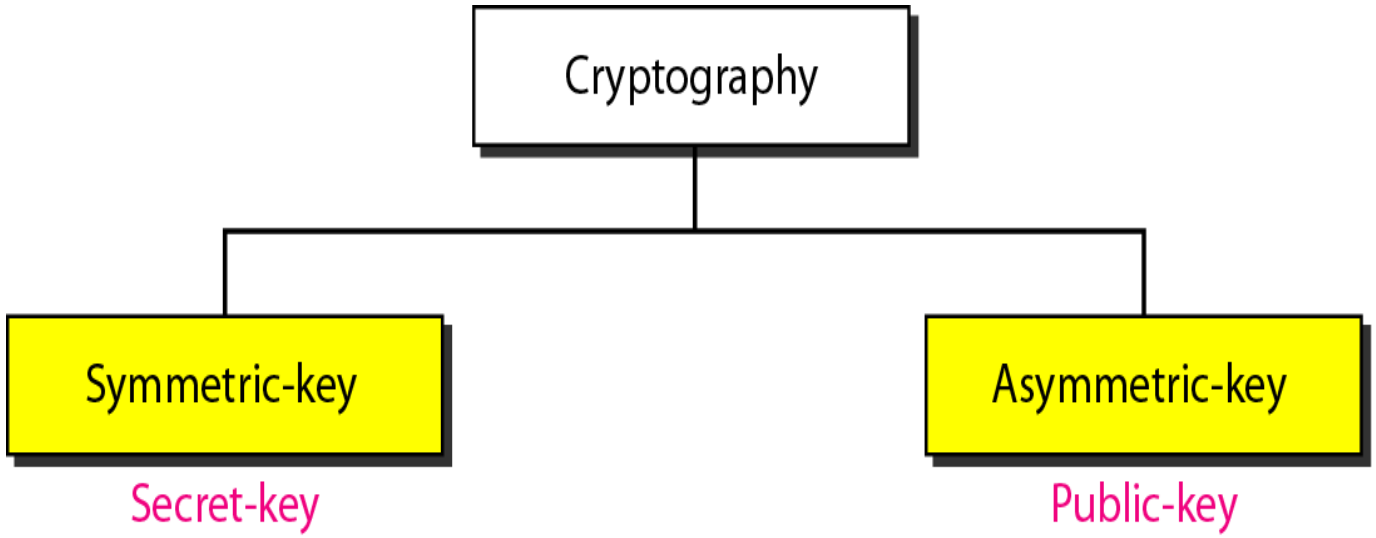
Introdução

- Componentes da Criptografia
  - Texto claro ou Texto aberto
  - Texto cifrado (texto criptografado)
  - Cifra (Algoritmo)
  - Chave



Introdução

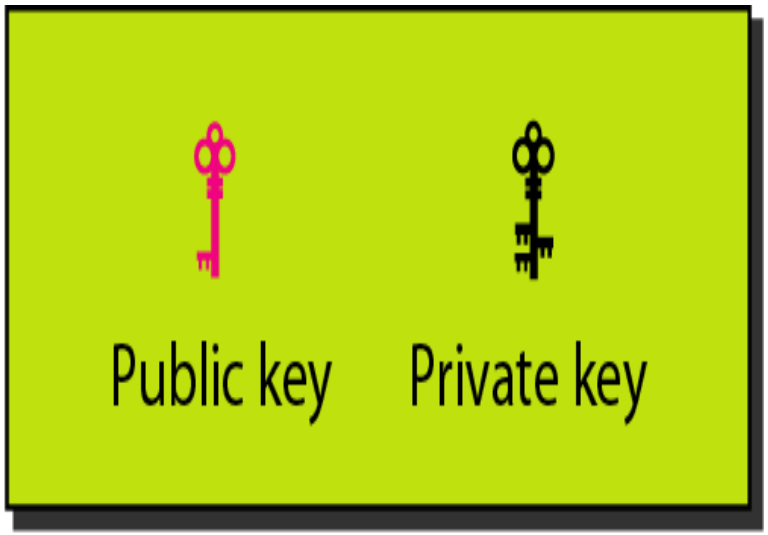
- Categorias da criptografia
  - Chave Simétrica (Chave Secreta)
  - Chave Assimétrica (Chave Pública)



Introdução

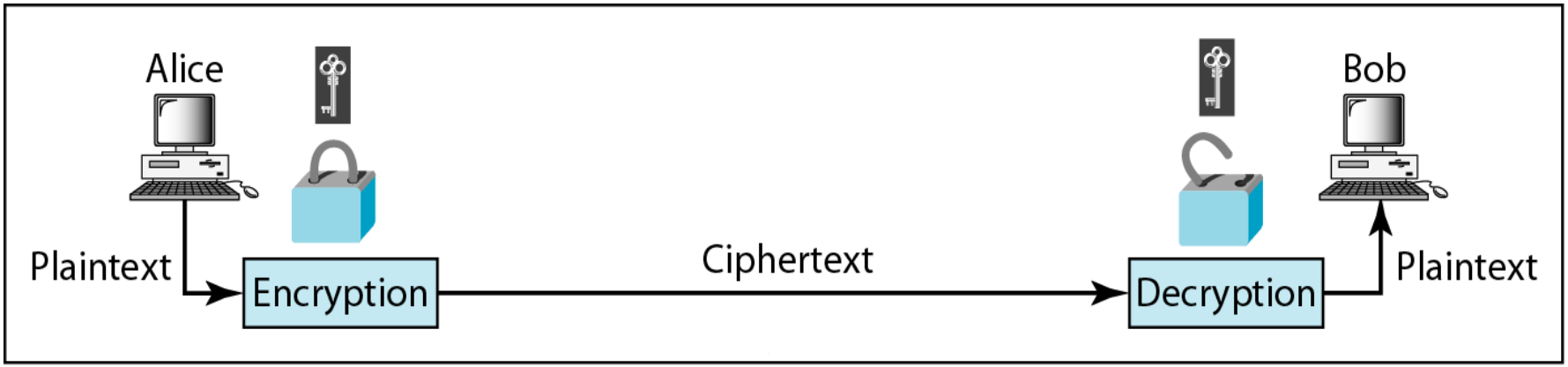
- Três tipos de chaves

Symmetric-key cryptography

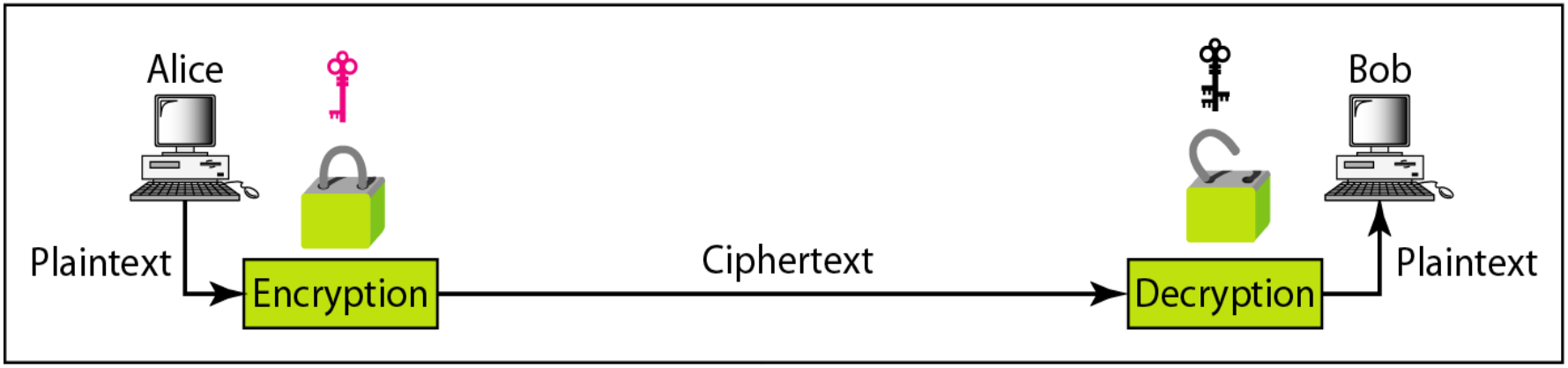


Asymmetric-key cryptography

Introdução



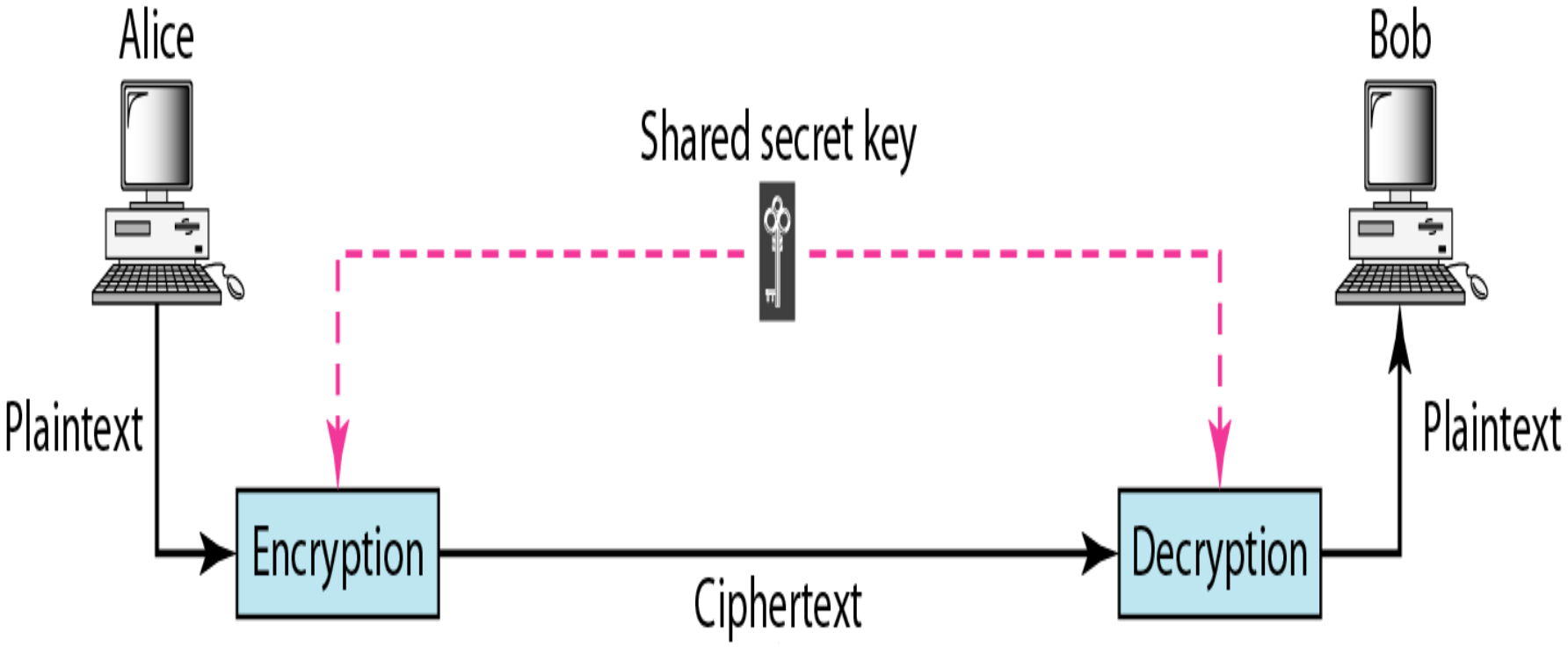
a. Symmetric-key cryptography



b. Asymmetric-key cryptography

Criptografia de Chave Simétrica

- Mesma chave utilizada por ambas as partes

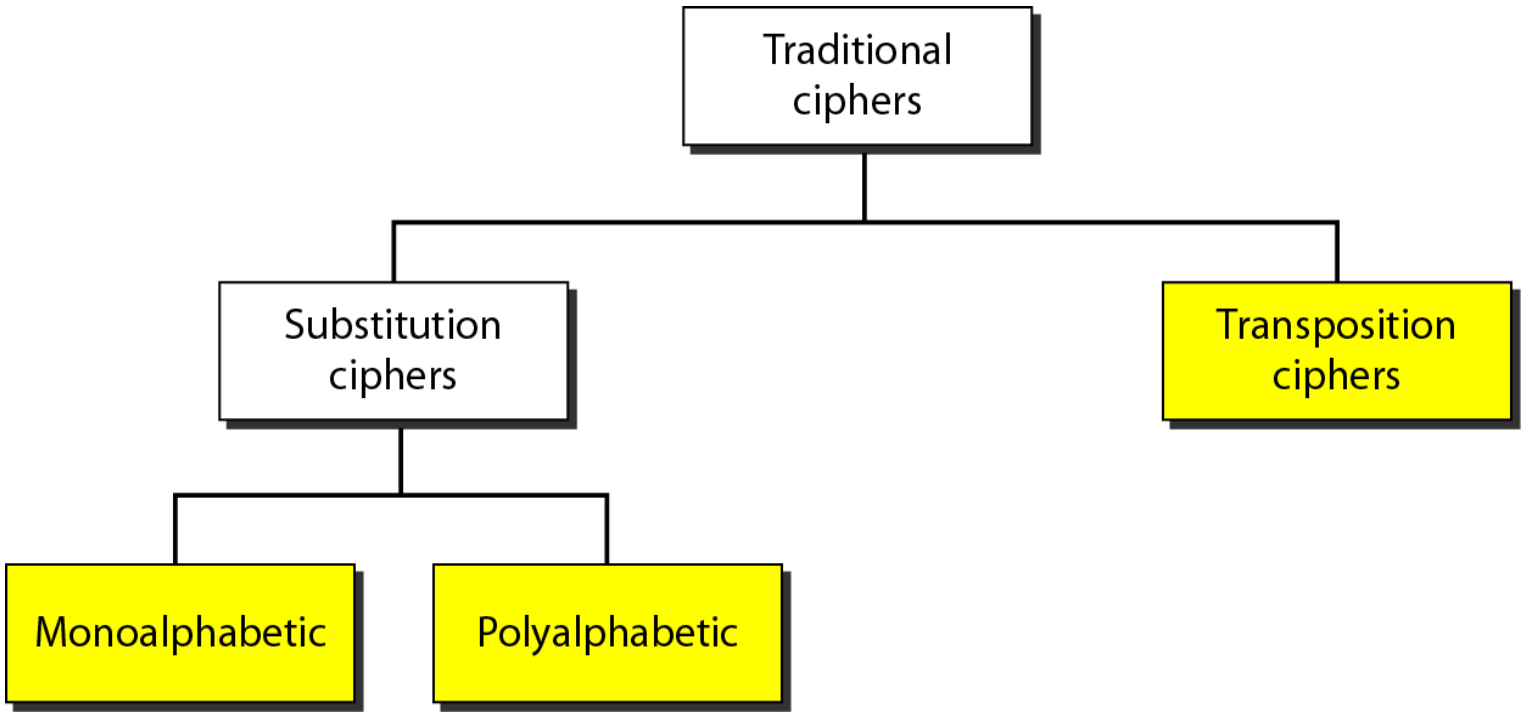


Criptografia de Chave Simétrica

- Iniciou a milhares de anos, quando as pessoas precisavam trocar segredos.
- Usado basicamente em segurança de redes.
- Cifras de hoje são muito mais completas
- Três categorias de cifras de chave simétrica:
  - Cifras Tradicionais
  - Cifras Modernas Simples
  - Cifras Cíclicas Modernas

Criptografia de Chave Simétrica

- **Cifras Tradicionais**
  - Cifras de Substituição
  - Cifras de Transposição



Criptografia de Chave Simétrica

Cifras Tradicionais de Substituição:

- Cifra Monoalfabética
  - Um caractere ou símbolo no texto claro sempre é modificado para o mesmo caractere ou símbolo no texto cifrado, independente de sua posição no texto. A relação entre os caracteres no texto claro e no texto cifrado é de um para um.
- Cifra Polialfabética
  - Cada ocorrência de um caractere pode ter um substituto diferente. A relação entre o caractere no texto claro para um caractere no texto cifrado é de um para vários.

Exemplo 1

- A cifra abaixo é monoalfabética?

Plaintext: HELLO
Ciphertext: KHOOR

  - Solução: Provavelmente é monoalfabética pois ambas as ocorrências da letra L são criptografadas com a letra O.

Exemplo 2

- A cifra abaixo é monoalfabética?

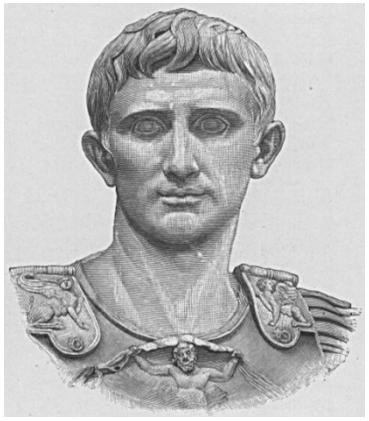
Plaintext: HELLO
Ciphertext: ABNZF

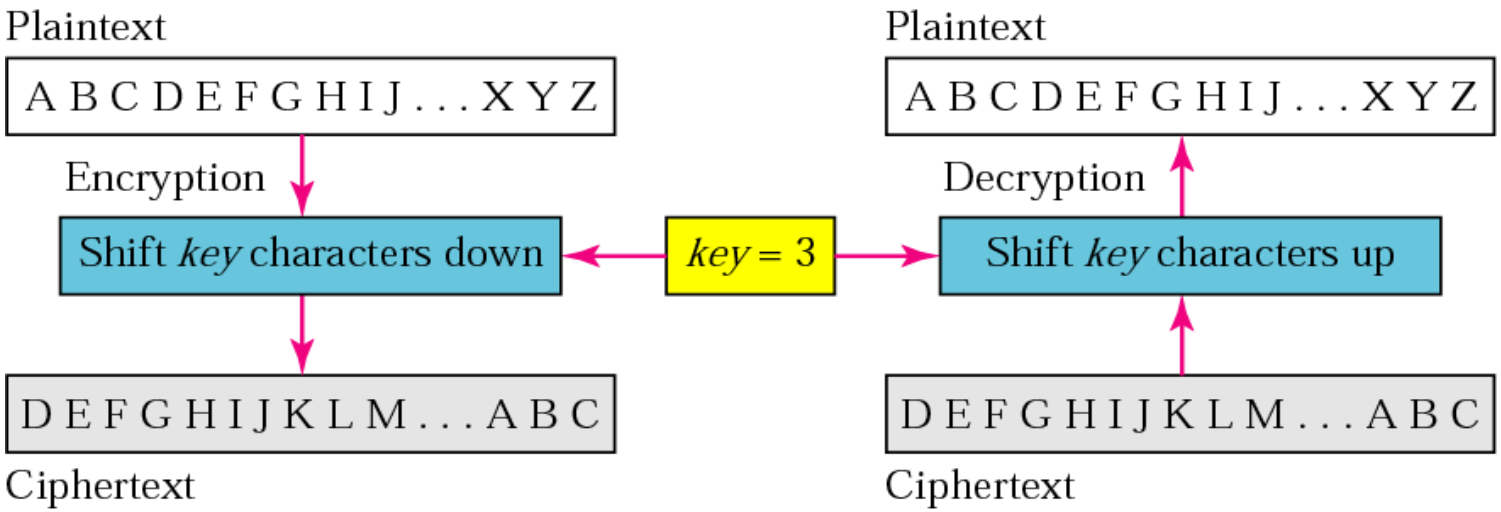
  - Solução: A cifra não é monoalfabética porque cada ocorrência da letra L é criptografada por um caractere diferente. A primeira letra L é criptografada como N; a segunda como Z.

Criptografia de Chave Simétrica

Cifras Tradicionais de Substituição (2):

- Cifra com Deslocamento
  - A cifra monoalfabética mais simples talvez seja a cifra com deslocamento. Nesse algoritmo é “deslocado **chave** caracteres para baixo”, em que a **chave** é igual a algum número. O algoritmo de decriptografia é “deslocado **chave** caracteres para cima”.
  - Algumas vezes é chamada de **Cifra de César**
  - Cifra de César (K = 3)
    - K-ésima letra sucessiva




Plaintext
A B C D E F G H I J . . . X Y Z
Encryption
Shift key characters down
key = 3
D E F G H I J K L M . . . A B C
Ciphertext
Plaintext
A B C D E F G H I J . . . X Y Z
Decryption
Shift key characters up
D E F G H I J K L M . . . A B C
Ciphertext

Exemplo 3

- Use a cifra com deslocamento de chave = 15 para criptografar a mensagem “HELLO”.
  - Solução: Criptografamos um caractere por sua vez. Cada caractere é deslocado 15 caracteres para baixo. A letra H é criptografada na letra W. A letra E é criptografada em T. O primeiro L é criptografado em A. O segundo L também é criptografado em A. E O é criptografado em D. O texto cifrado fica WTAAD.

Exemplo 4

- Use cifra com deslocamento com chave = 15 para decriptografar a mensagem “WTAAD”.
  - Solução: Decriptografamos um caractere por vez. Cada caractere é deslocado 15 para cima. A letra W é decriptografada em H. A letra T é decriptografada em E. O primeiro A é decriptografada em L. O segundo A é em L; e, finalmente, o D é em O. O texto claro é HELLO.

Exemplo 5

- Criptografia polialfabética
  - Duas cifras de César (k = 5 e k = 19)
  - A mensagem em texto aberto é SEGURANCA
  - O modelo de repetição é C1, C2, C2, C1, C2.

	a	b	c	d	e	f	g	h	i	f	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C1:	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
C2:	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s

  - Solução: XXZZKFGVF

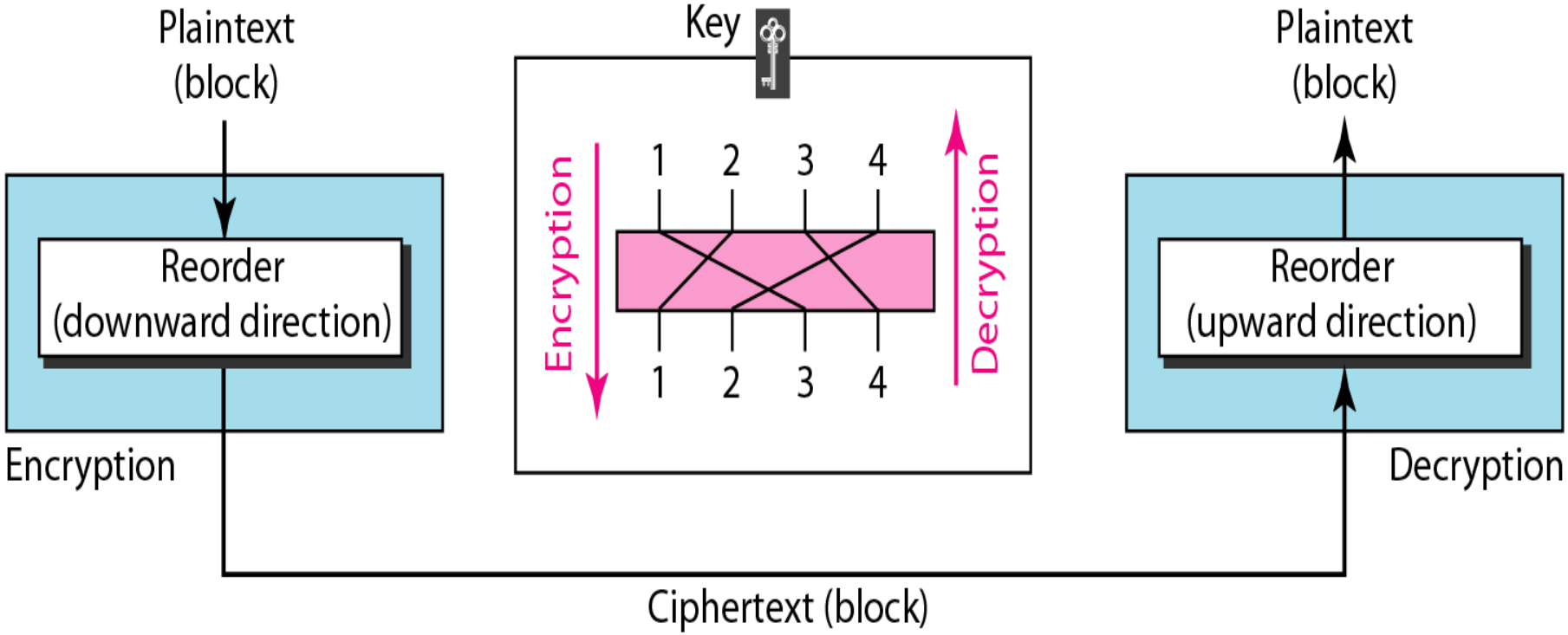
Criptografia de Chave Simétrica

Características da Cifra de César:

- Apresenta 25 pares possíveis. O aprimoramento apresenta 26.
- 10^{26} pares possíveis.
- E e T aparecem em 22% dos textos em inglês.
- Três cenários de possíveis ataques
  - Ataque exclusivo a texto cifrado
  - Ataque com texto aberto conhecido
  - Ataque com texto aberto escolhido,
    - Ex: “The quick fox jumps over the lazy brown dog”

Criptografia de Chave Simétrica

- Cifras de Transposição
  - Reordena (permuta) símbolos em um bloco de símbolos.



Exemplo 6

- Criptografe a mensagem “HELLO MY DEAR” usando a chave citada.
  - Solução: Primeiro eliminamos os espaços na mensagem. Em seguida, dividimos o texto em blocos de quatro caracteres. Adicionamos um caractere falso Z no final do terceiro bloco. O resultado é HELL OMYD EARZ. Criamos um texto cifrado de três blocos, ELHLMDOYAZER.

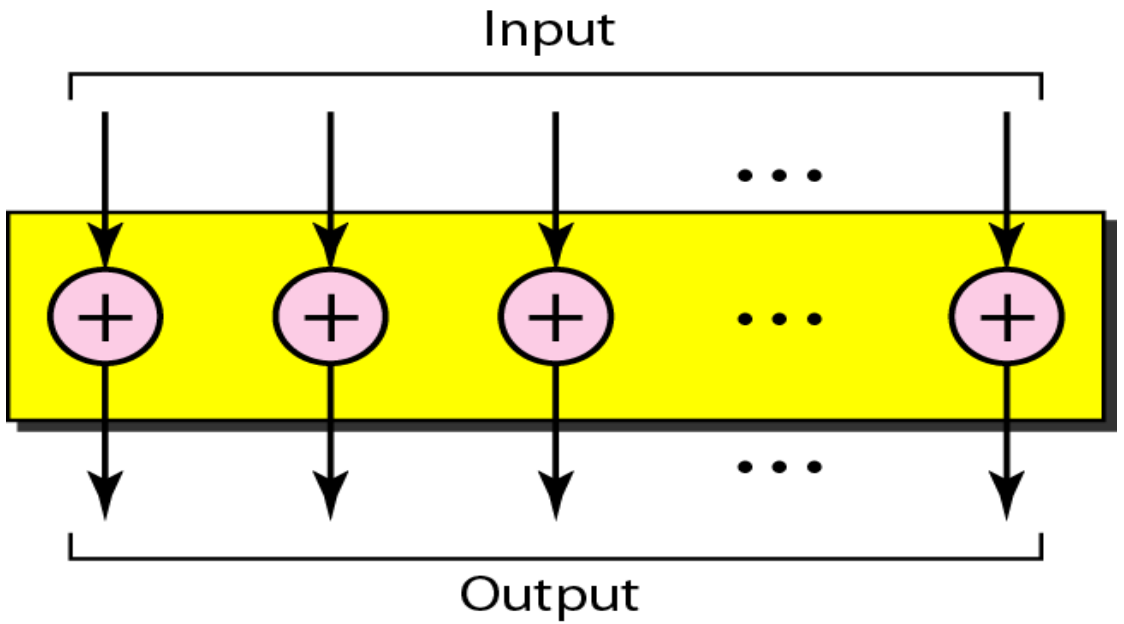
Exemplo 7

- Decriptografe a mensagem “ELHLMDOYAZER”.
  - Solução: O resultado é HELL OMYD EARZ . Após eliminar o caractere falso (Z) e combinar os caracteres, obtemos a mensagem original “HELLO MY DEAR”.

Criptografia de Chave Simétrica

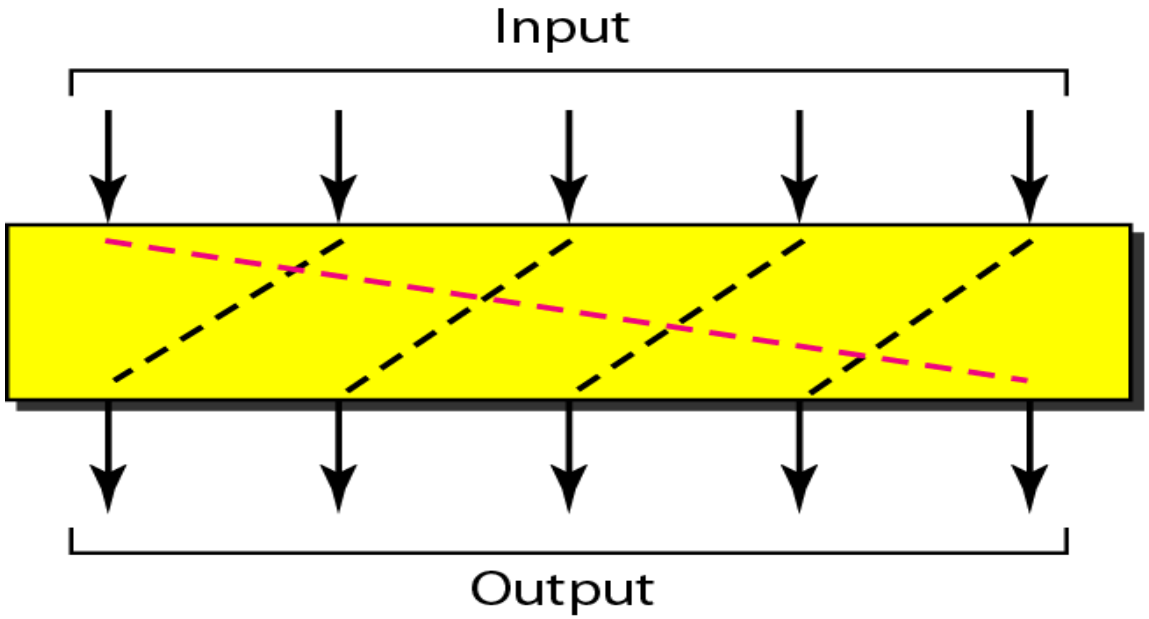
Cifras Modernas Simples:

- **Cifra XOR**
  - Usa a operação ou-exclusivo, conforme definido na computação.



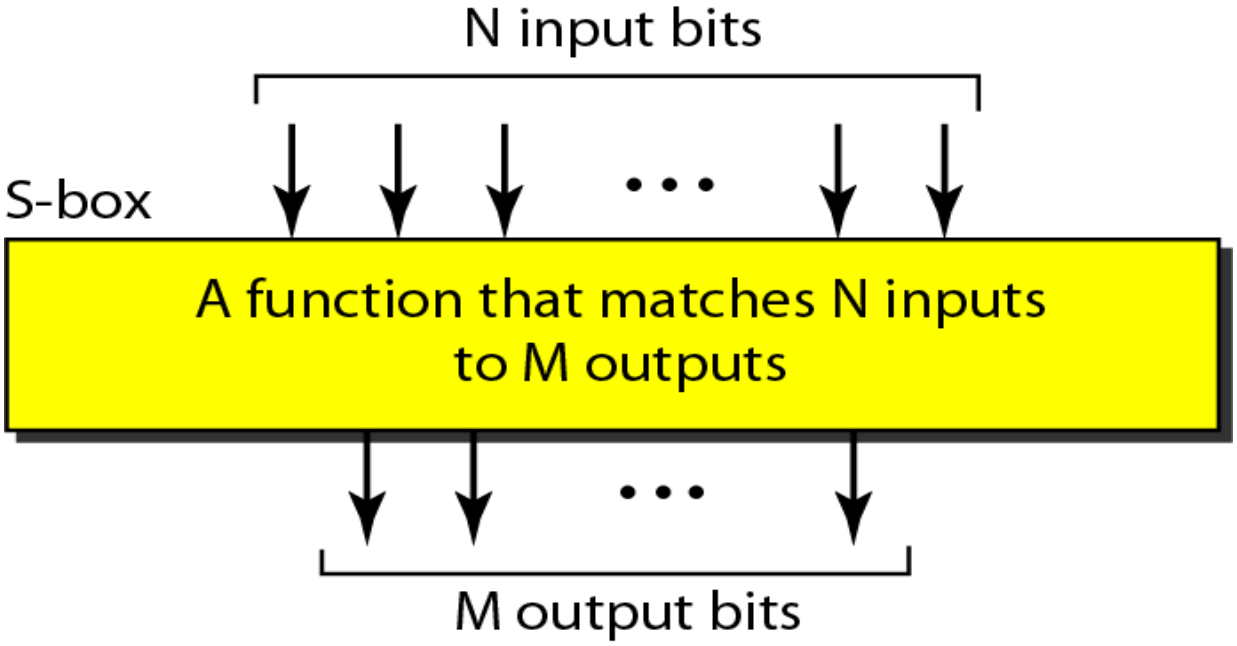
Criptografia de Chave Simétrica

- **Cifra de Rotação**
  - Nessa cifra, os bits de entrada são deslocados para a esquerda ou para a direita, podendo ser com ou sem chaves.



Criptografia de Chave Simétrica

- **Cifra de Substituição: S-box**
  - Análogo da cifra de substituição para caracteres. A entrada é um fluxo de bits de comprimento N; a saída é outro fluxo de bits de comprimento M.

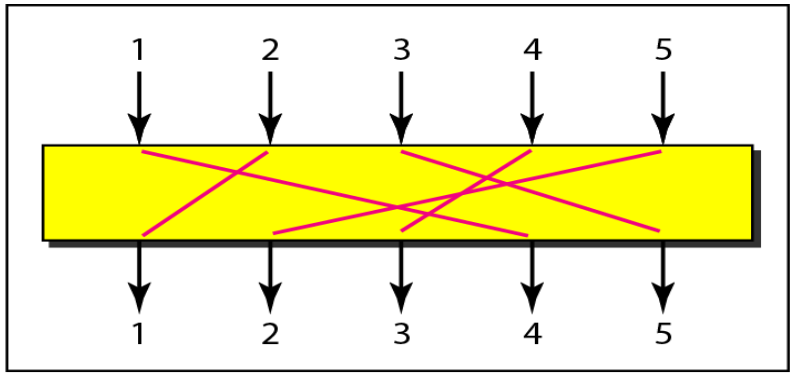


Criptografia de Chave Simétrica

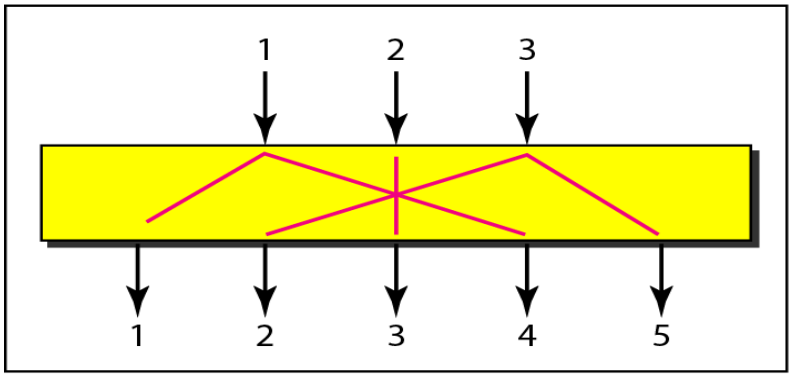
- **Cifra de Transposição: P-box**
  - É um análogo da cifra de transposição tradicional para caracteres, realizando uma transposição em termo de bits; ela transpõe bits (permutação).

Criptografia de Chave Simétrica

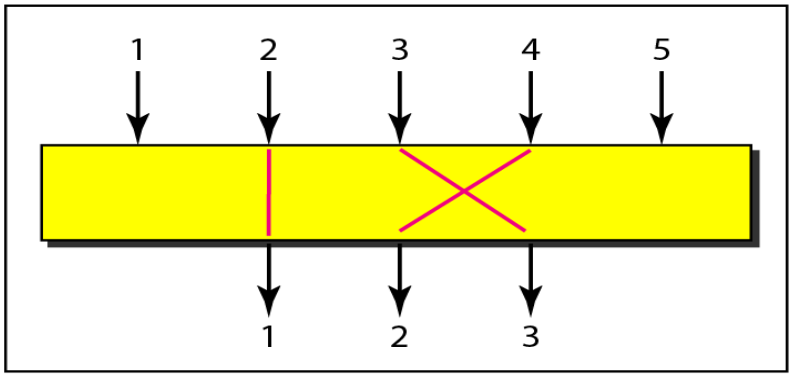
- **Cifra de Transposição: P-box**



a. Straight



b. Expansion



c. Compression

Criptografia de Chave Simétrica

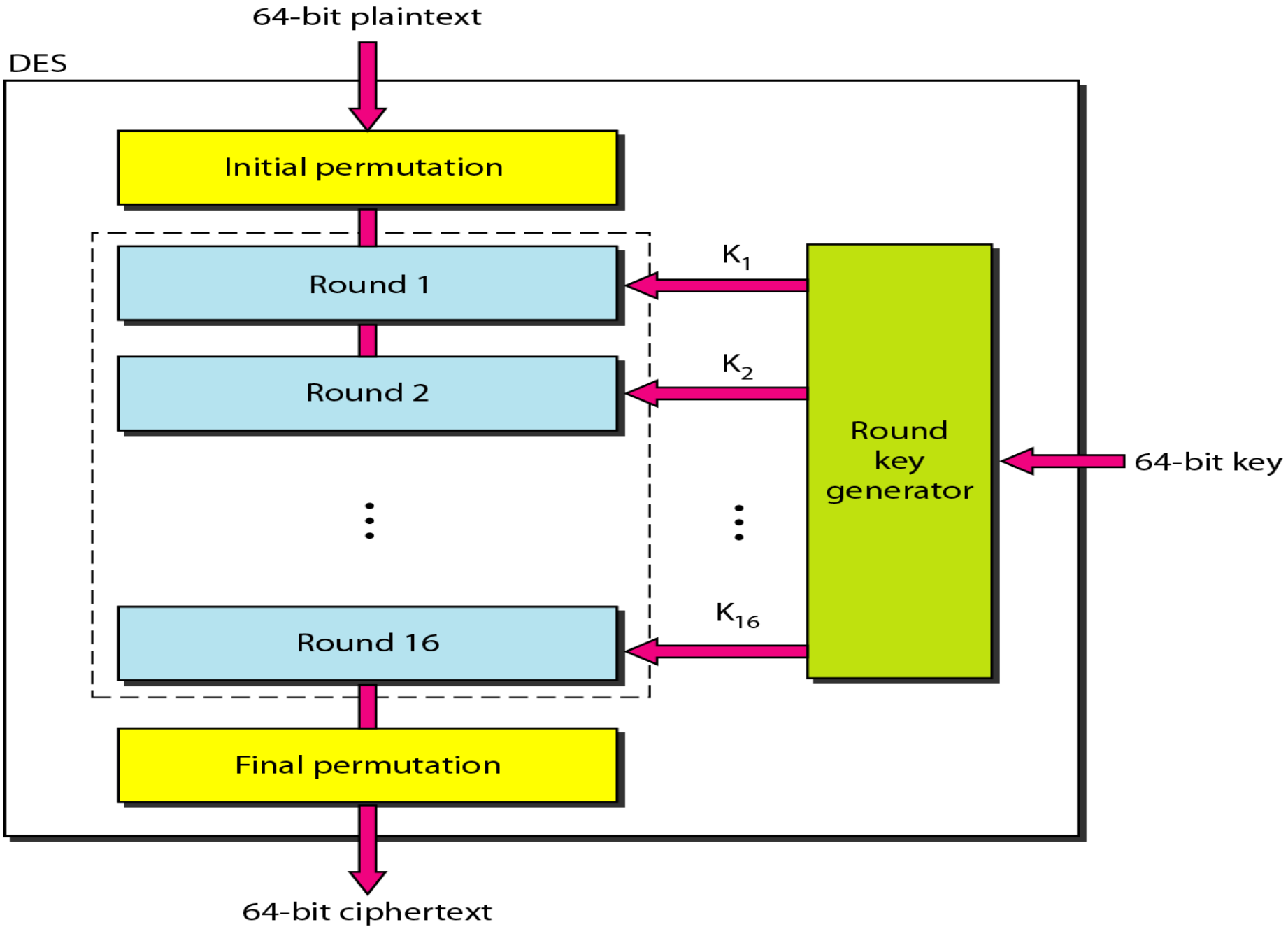
Cifras Cíclicas Modernas

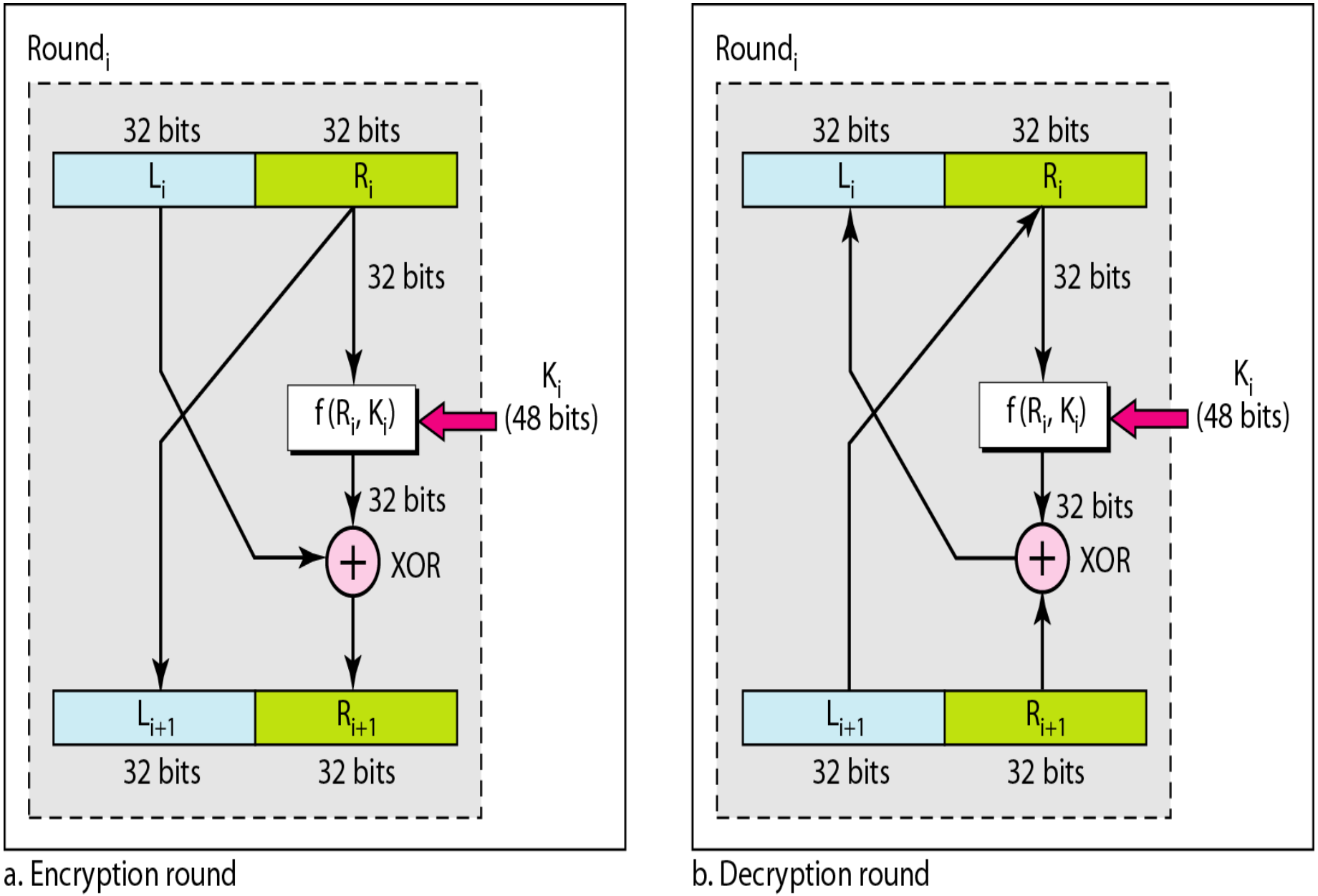
- Abordaremos duas cifras de chaves simétricas modernas
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)

Criptografia de Chave Simétrica

Padrão de Criptografia de Dados

- Um exemplo de cifras de blocos complexa é o DES (Data Encryption Standard).
- O algoritmo criptografa um bloco de texto claro de 64 bits usando uma chave de 64 bits.

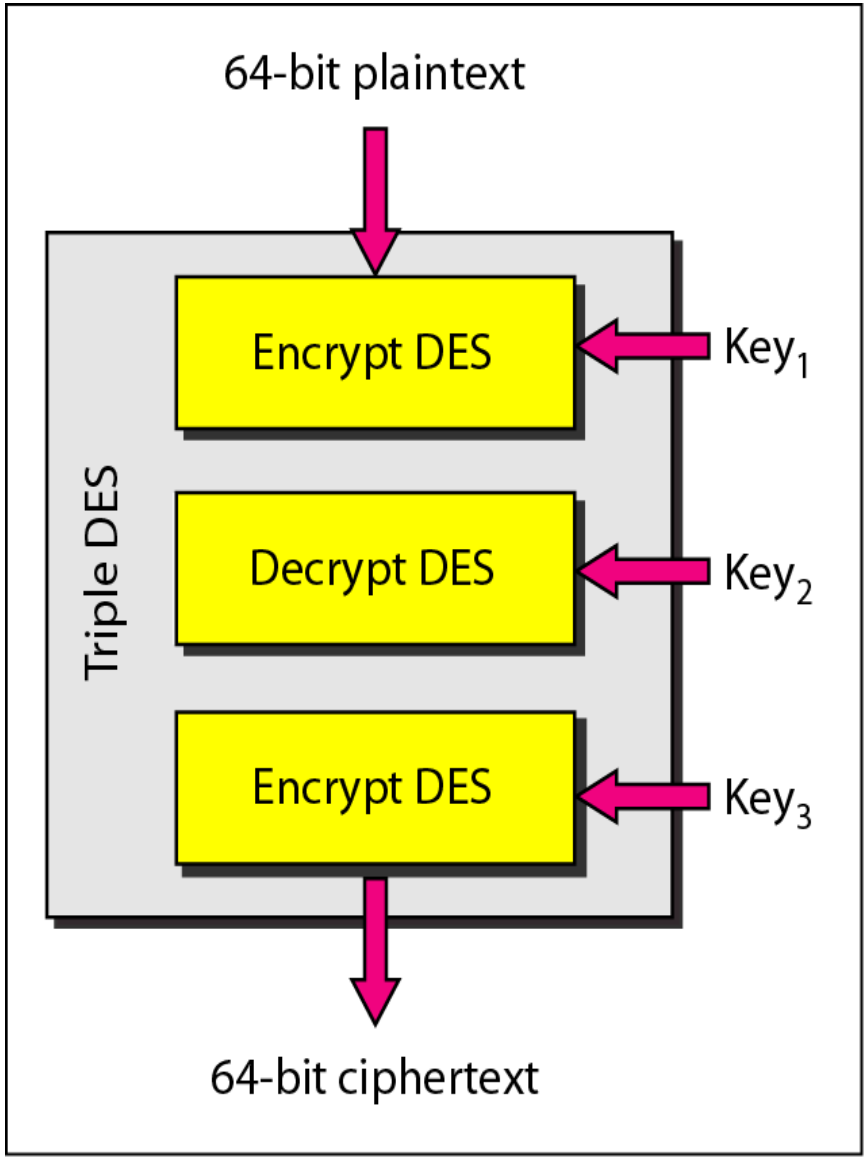

64-bit plaintext
DES
Initial permutation
Round 1
Round 2
Round 16
Final permutation
64-bit ciphertext
K1
K2
K16
Round key generator
64-bit key


Round$_i$
32 bits
32 bits
L_i
R_i
32 bits
K_i
(48 bits)
$f(R_i, K_i)$
32 bits
XOR
L_{i+1}
R_{i+1}
32 bits
32 bits
a. Encryption round
Round$_i$
32 bits
32 bits
L_i
R_i
32 bits
K_i
(48 bits)
$f(R_i, K_i)$
32 bits
XOR
L_{i+1}
R_{i+1}
32 bits
32 bits
b. Decryption round

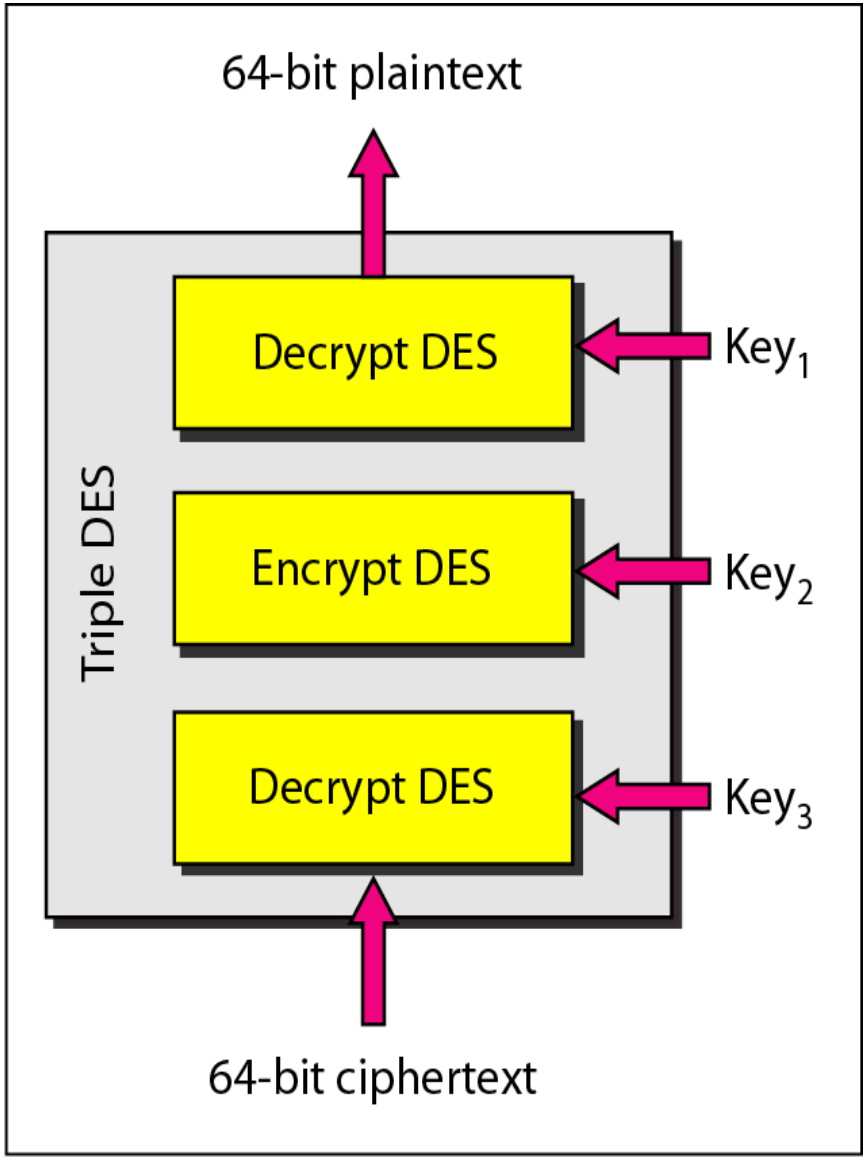
Criptografia de Chave Simétrica

DES é seguro?

- Recebeu muitas críticas devido ao tamanho da chave
- 1997 (DES Challenge) – 4 meses
- 1999 (DES Challenge III) – 22 horas (Deep Crack)
- Triple DES (Triplo DES ou 3DES)
- Com duas chaves (Chave 1 = Chave 3)
  - Chaves com 112 bits
- Com três chaves
  - Chaves com 168 bits



a. Encryption Triple DES



b. Decryption Triple DES

Criptografia de Chave Simétrica

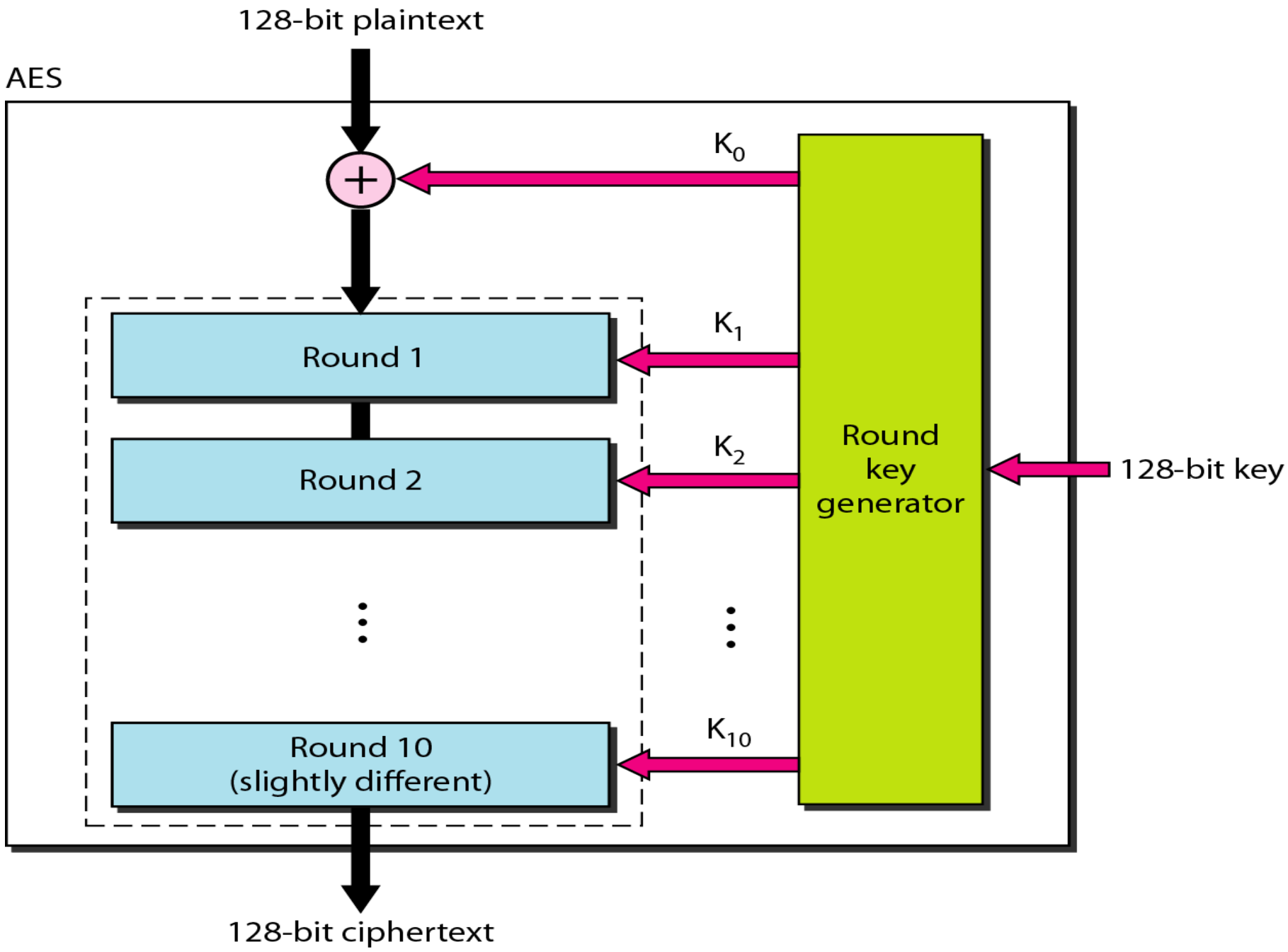
Padrão de Criptografia Avançado

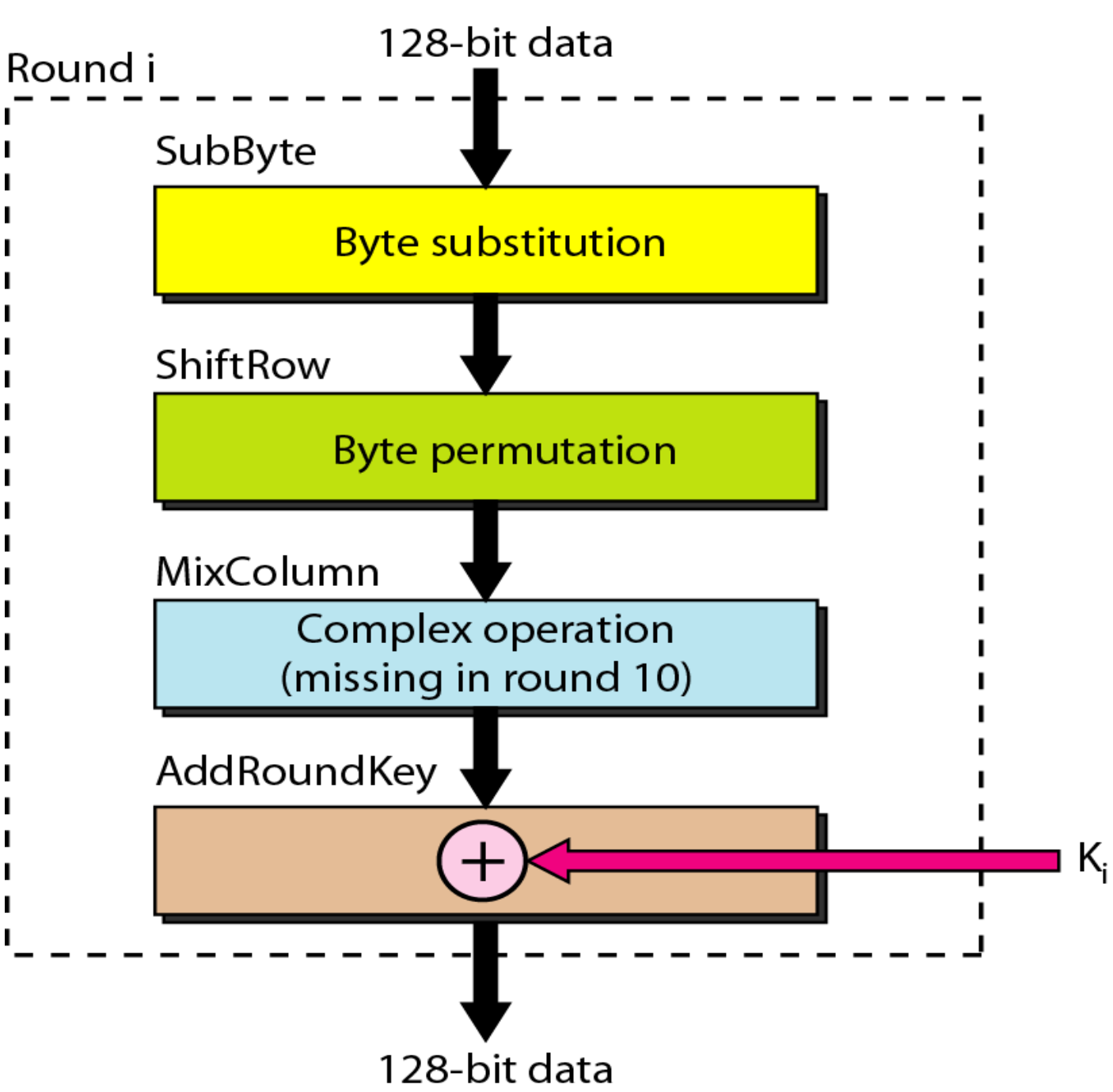
- AES (Advanced Encryption Standard)
  - Concebido devido ao tamanho da chave DES ser muito pequena.
  - Embora o triplo DES (3DES) aumentasse o tamanho da chave, o processo era muito lento.
  - O AES é uma cifra cíclica muito complexa e foi projetado com três tamanhos de chave: 128, 192 e 256 bits.

Criptografia de Chave Simétrica

- AES (Advanced Encryption Standard)
  - NIST (National Institute of Standards and Technology) optou pelo algoritmo Rinjdael como base do AES.

Size of Data Block	*Number of Rounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

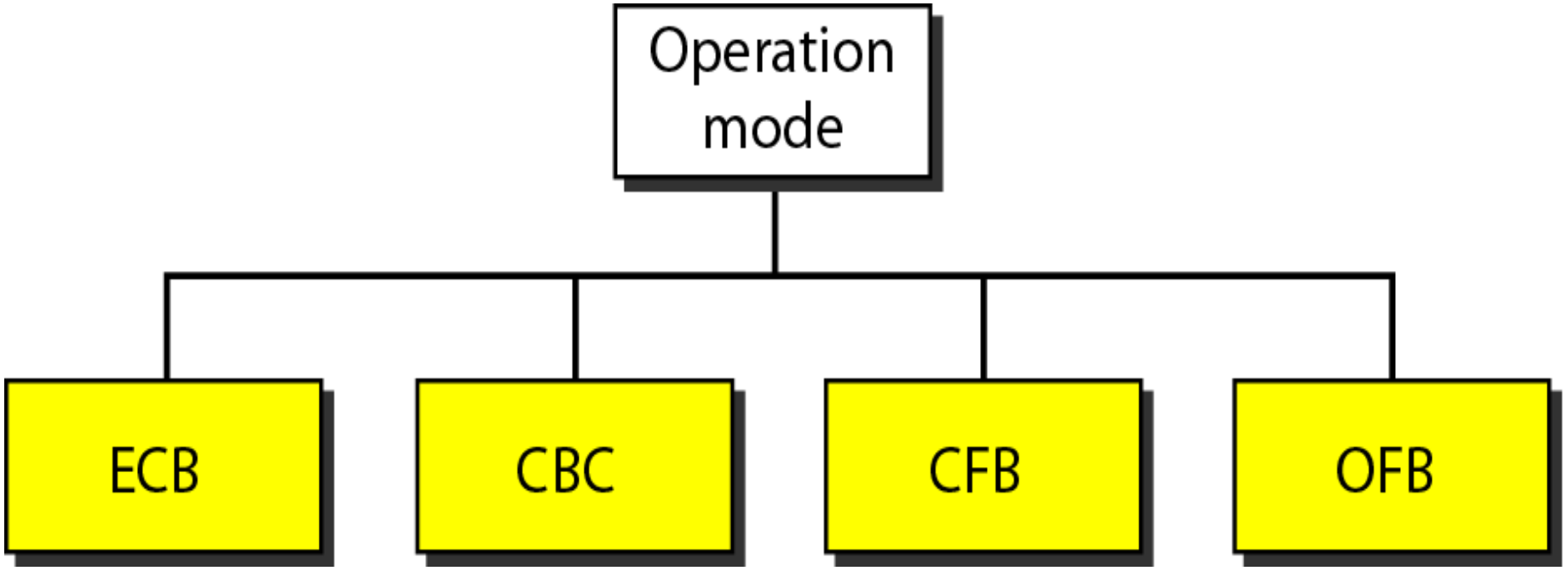

128-bit plaintext
AES
K_0
K_1
K_2
K_{10}
Round 1
Round 2
Round 10
(slightly different)
Round
key
generator
128-bit key
128-bit ciphertext


Round i
128-bit data
SubByte
Byte substitution
ShiftRow
Byte permutation
MixColumn
Complex operation
(missing in round 10)
AddRoundKey
+
K_i
128-bit data

Criptografia de Chave Simétrica

Modo de Operação

- É uma técnica que emprega as modernas cifras de blocos como DES e AES.



Criptografia de Chave Simétrica

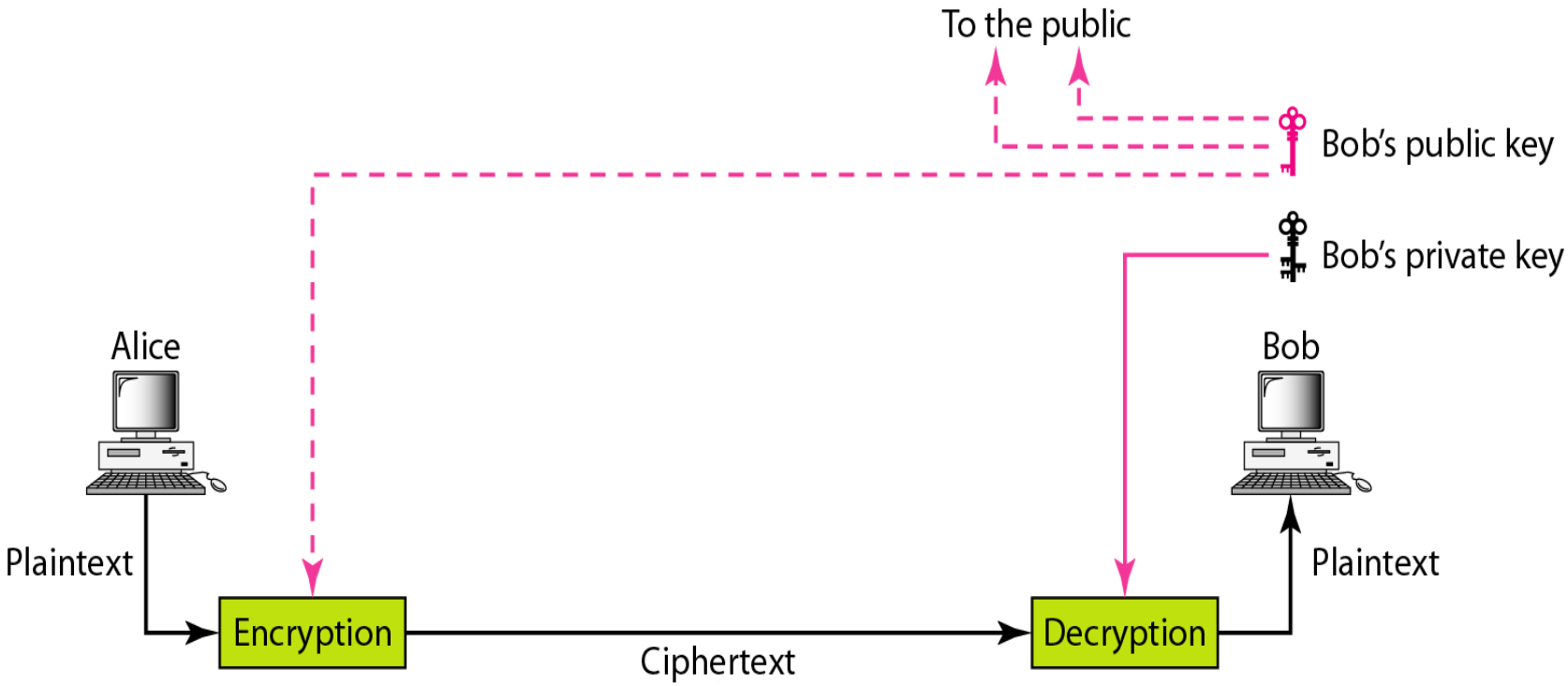
- **EBC (Electronic Code Book)** – É uma técnica que se baseia puramente em cifras de blocos. O texto claro é dividido em blocos de N bits. O texto cifrado é formado por blocos de N bits. O valor de N depende do tipo de cifra usada.
- **CBC (Cipher Block Chaining)** – Tenta minimizar parte dos problemas do ECB incluindo blocos de cifra anterior na preparação do bloco atual.

Criptografia de Chave Simétrica

- **CFB (Cipher Feedback)** – Criado para aquelas situações nas quais precisamos receber ou enviar r bits de dados, em que r é um número diferente do tamanho do bloco da cifra de criptografia usada.
- **OFB (Output Feedback)** – Similar ao modo CFB com apenas uma diferença. Cada bit no texto cifrado é independente do bit ou bits anteriores. Isso impede a propagação de erros. Se ocorrer um erro de transmissão, ele não afeta os bits futuros.

Criptografia de Chave Assimétrica

- Existem duas chaves
  - Chave Privada
  - Chave Pública



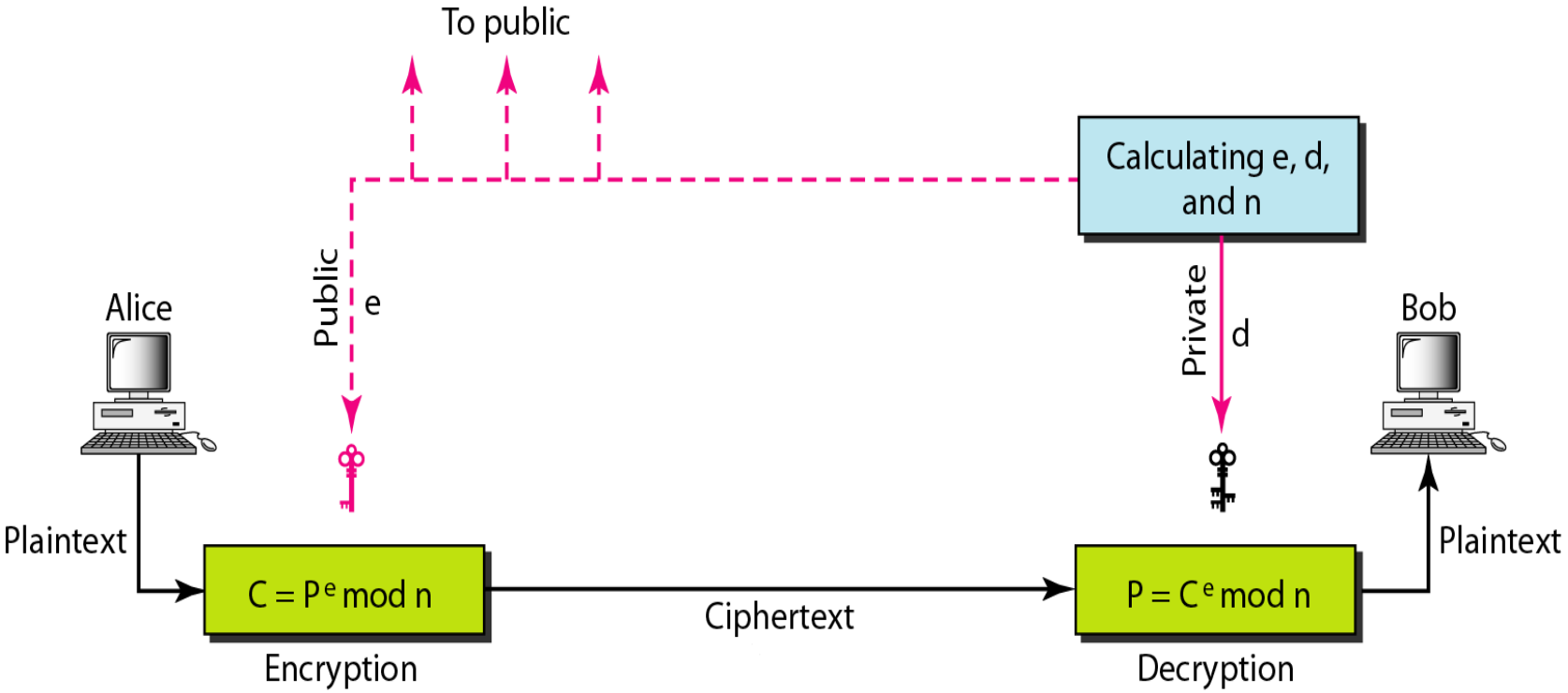
Criptografia de Chave Assimétrica

- Nesse tipo de criptografia, discutiremos dois algoritmos:
  - RSA
  - Diffie-Hellman

Criptografia de Chave Assimétrica

RSA (*Rivest, Shamir e Adleman*)

- Usa dois números, *e* e *d* conforme mostrado abaixo



Criptografia de Chave Assimétrica

- Bob usa as seguintes etapas para selecionar as chaves privada e pública:
  1. Escolhe dois números primos muito grandes, *p* e *q.*
  2. Multiplica os dois primos escolhidos para descobrir *n*, o módulo para criptografia e decriptografia. Em outras palavras, n = p x q.
  3. Calcula outro número $\Phi = (p - 1) \times (q - 1)$.
  4. Escolhe um número inteiro aleatório *e*. Em seguida, calcula *d* de modo que $(d - e^{-1})$ seja um múltiplo de Φ ($d = e^{-1} \bmod \Phi$) (Ex.: 38 = 2mod12 (38-2=36)))
  5. Anuncia *e* e *n* para o público; ele mantém Φ e *d* secretos.
- No RSA, *e* e *n* são anunciados ao público; *d* e Φ são mantidos secretos.

Exemplo 8

- Bob escolhe 7 e 11 como *p* e *q* e calcula *n* = 7 . 11 = 77.
- O valor de Φ = (7 – 1) (11 – 1) ou 60.
- Dessa vez, ele escolhe duas chaves, *e* e *d*.
- Se optar por *e* ser 13, então *d* é 37.

Plaintext: 5
$C = 5^{13} = 26 \bmod 77$
Ciphertext: 26

Ciphertext: 26
$P = 26^{37} = 5 \bmod 77$
Plaintext: 5

Exemplo 8

- Imagine agora Alice enviando o texto claro 5 para Bob.
- Ela usa a chave pública 13 para criptografar e 5. Bob recebe o texto cifrado 26 e usa a chave privada 37 para decifrar o texto cifrado.

Plaintext: 5
$C = 5^{13} = 26 \bmod 77$
Ciphertext: 26

Ciphertext: 26
$P = 26^{37} = 5 \bmod 77$
Plaintext: 5

Criptografia de Chave Assimétrica

Diffie-Hellman

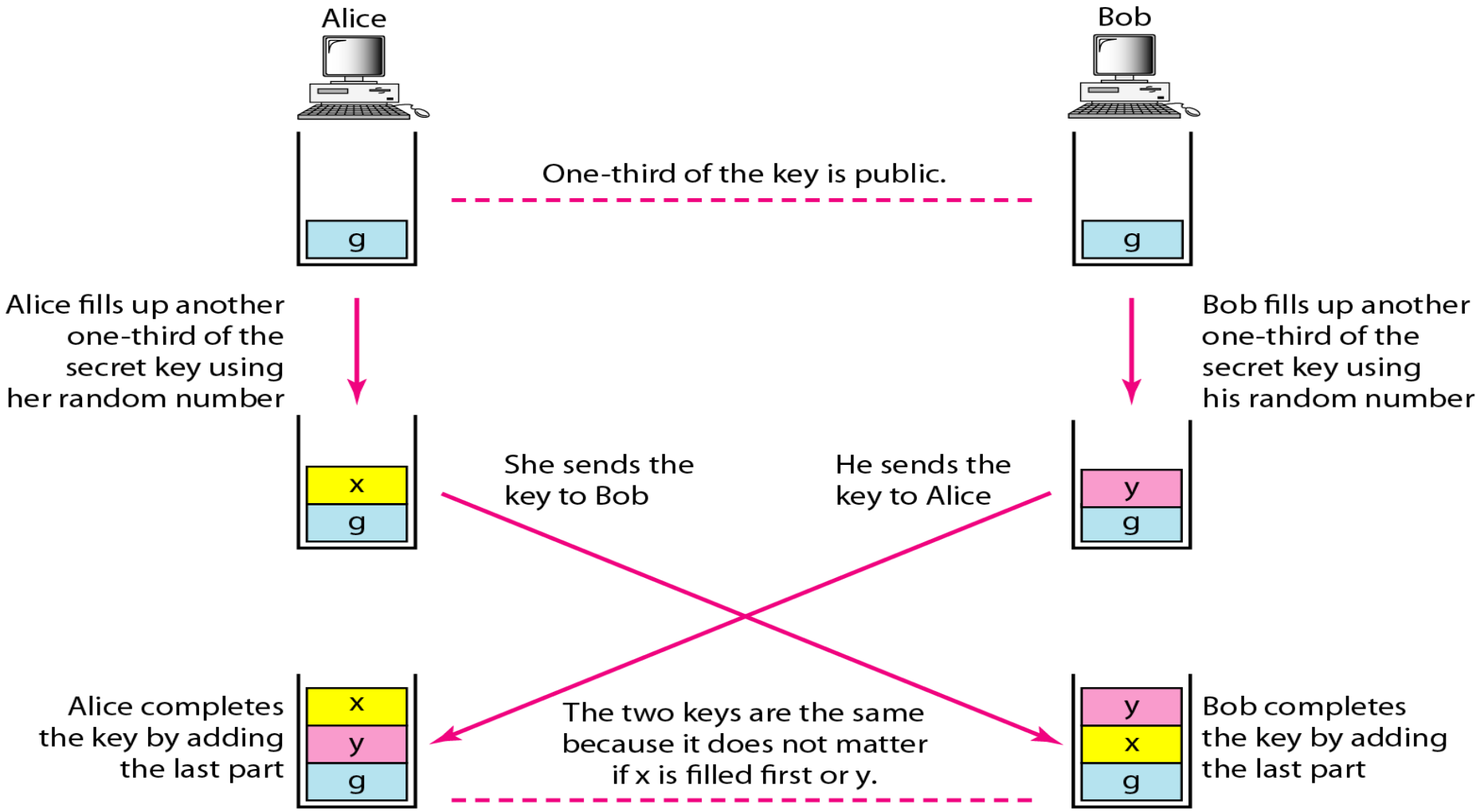
- Neste criptosistema, duas partes criam uma chave de sessão simétrica para troca de dados sem ter de se lembrar ou armazenar a chave para uso futuro. Eles não precisam se encontrar para chegar a um acordo sobre a chave.
- O método de Diffie-Hellman fornece uma chave de sessão por uma única vez para as duas partes.
- A chave simétrica compartilhada no protocolo Diffie-Hellman é $K = g^{xy} \bmod p$.

Criptografia de Chave Assimétrica

Diffie-Hellman (2)

- É um protocolo de criação de chaves simétricas muito sofisticado.
- Se *x* e *y* forem números muito grandes, é muito difícil para um intruso descobrir a chave conhecendo-se apenas p e g. Um invasor precisaria determinar *x* e *y* se R1 e R2 fossem interceptados.

Algoritmo de Diffie-Hellman

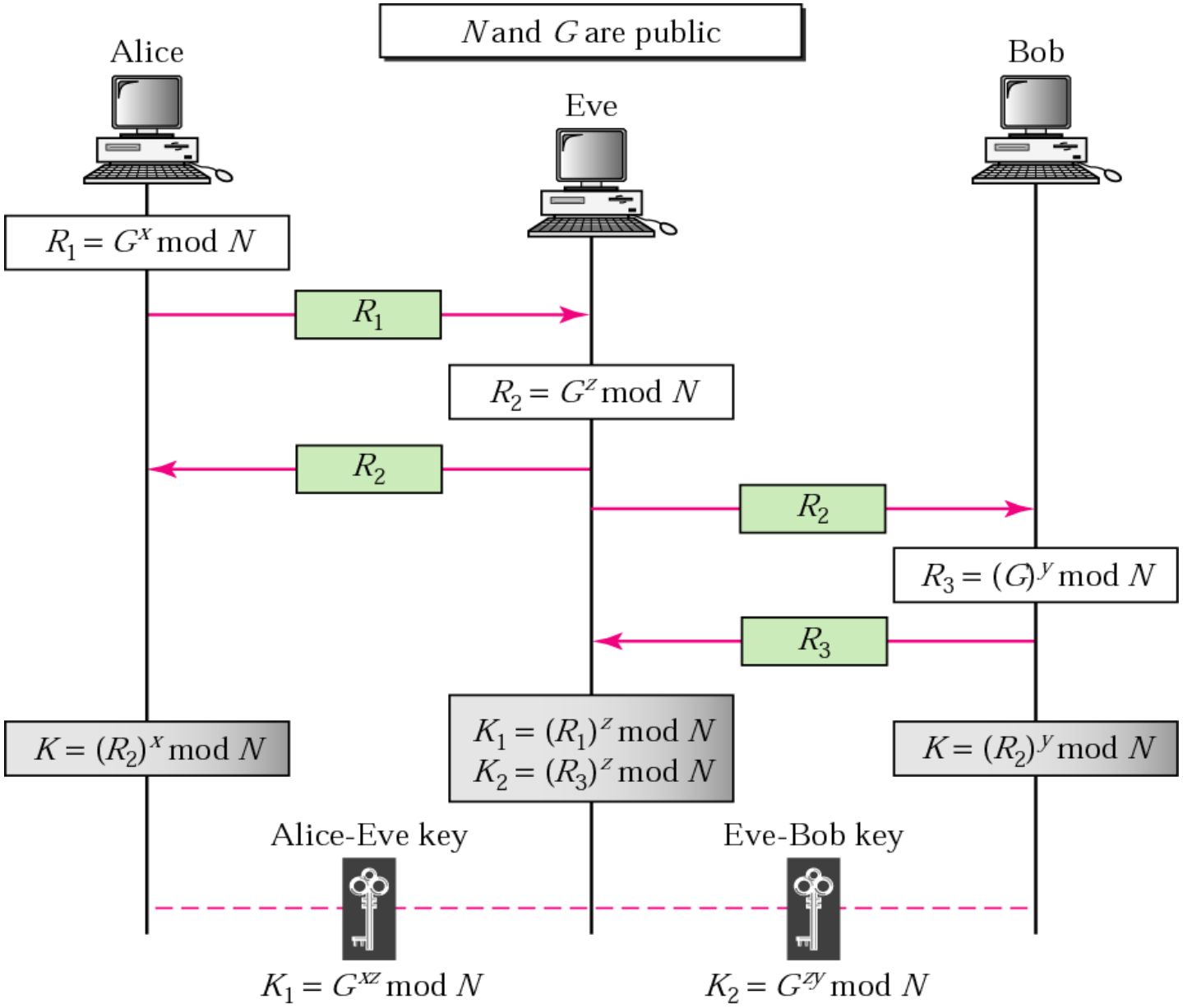


Algoritmo de Diffie-Hellman

- Vamos dar um exemplo para tornar o processo claro. Suponha G = 7 e N = 23. As etapas são as seguintes:
  1. Alice escolhe x = 3 e calcula R1 = 7^3 mod 23 = 21.
  2. Alice envia o número 21 para Bob.
  3. Bob escolhe y = 6 e calcula R2 = 7^6 mod 23 = 4.
  4. Bob envia o número de 4^3 a Alice.
  5. Alice calcula a chave simétrica K = 4^3 mod 23 = 18.
  6. Bob calcula a chave simétrica K = 21^6 mod 23 = 18.
- O valor de K é a mesma para ambos Alice e Bob, G^{xy} mod N = 718 mod 23 = 18.

Criptografia de Chave Assimétrica

- Ataque “Homem no Meio”
  - O intruso não tem de encontrar o valor de *x* e *y* para atacar o protocolo.
  - Pode enganar Alice e Bob criando duas chaves: uma entre ela e Alice e outra entre ela e Bob.


N and G are public
Alice
Eve
Bob
$R_1 = G^X \bmod N$
R_1
$R_2 = G^Z \bmod N$
R_2
R_2
$R_3 = (G)^Y \bmod N$
R_3
$K = (R_2)^X \bmod N$
$K_1 = (R_1)^Z \bmod N$
$K_2 = (R_3)^Z \bmod N$
$K = (R_2)^Y \bmod N$
Alice-Eve key
Eve-Bob key
$K_1 = G^{XZ} \bmod N$
$K_2 = G^{ZY} \bmod N$

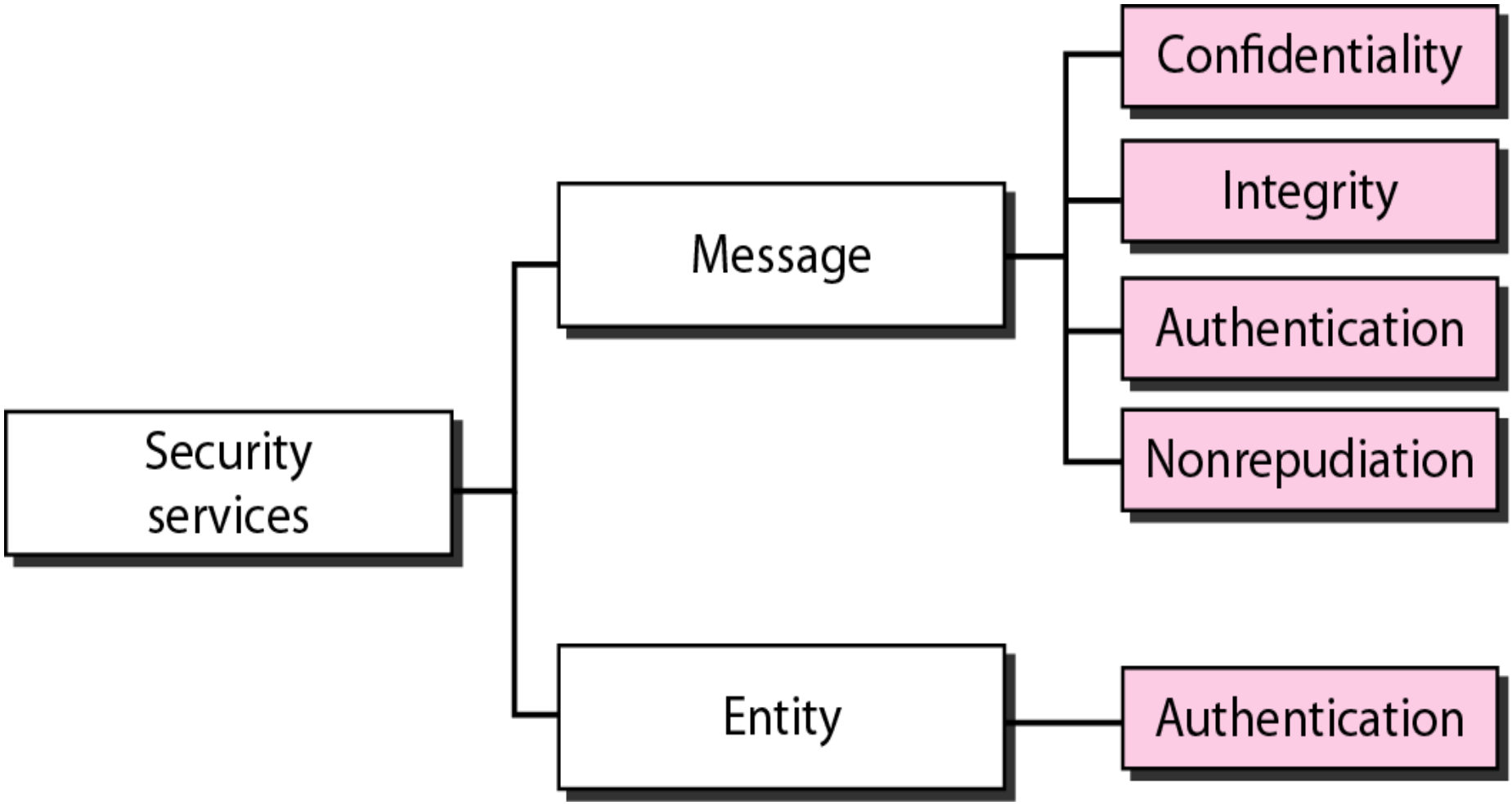
SEGURANÇA DE REDES

Introdução

O que é segurança na rede?

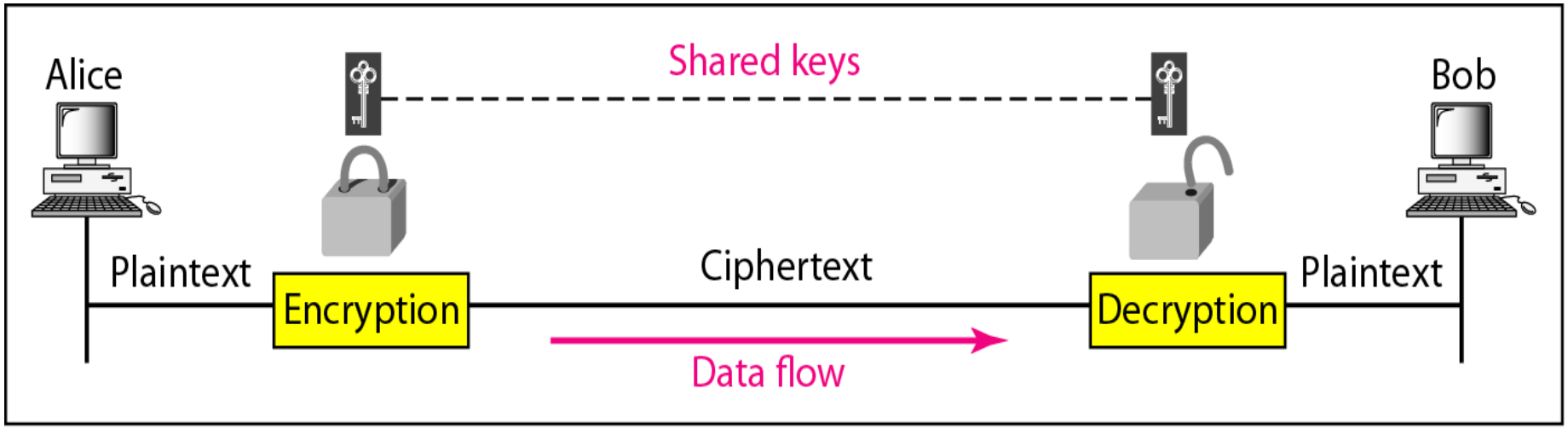
- Para que uma rede possa ser considerada segura, ninguém (exceto os envolvidos) pode **interceptar**, **ler** ou **executar** processos computacionais trocados entre os mesmos.
- Necessita-se prover Confidencialidade, Integridade, Autenticação e Não-Repúdio.
- Protocolos AAA (Authentication, Authorization, Accounting – Autenticação, Autorização, Contabilização)

Serviços de Segurança

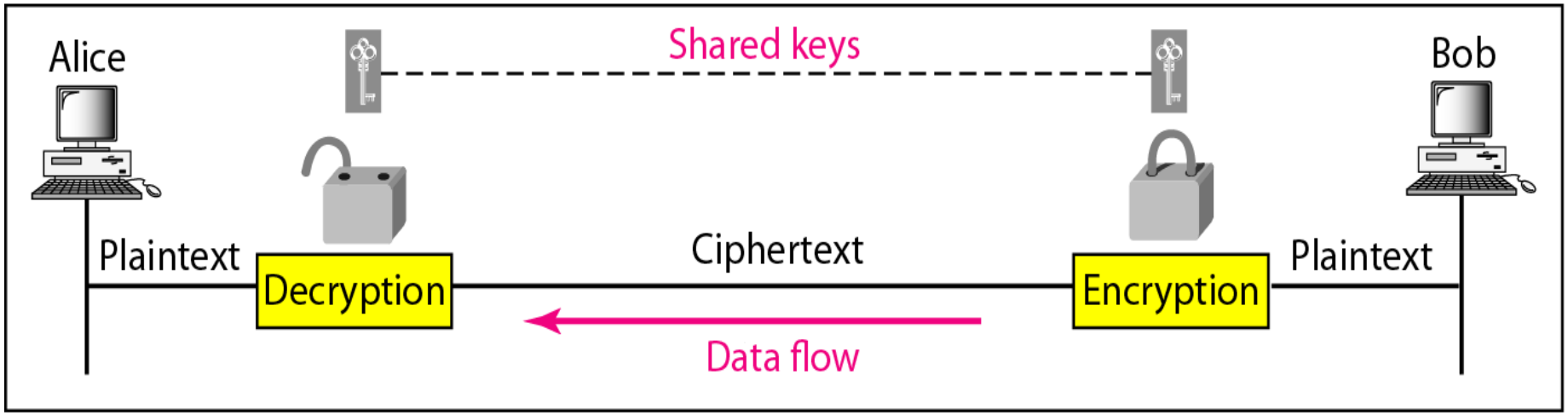


Confidencialidade da Mensagem

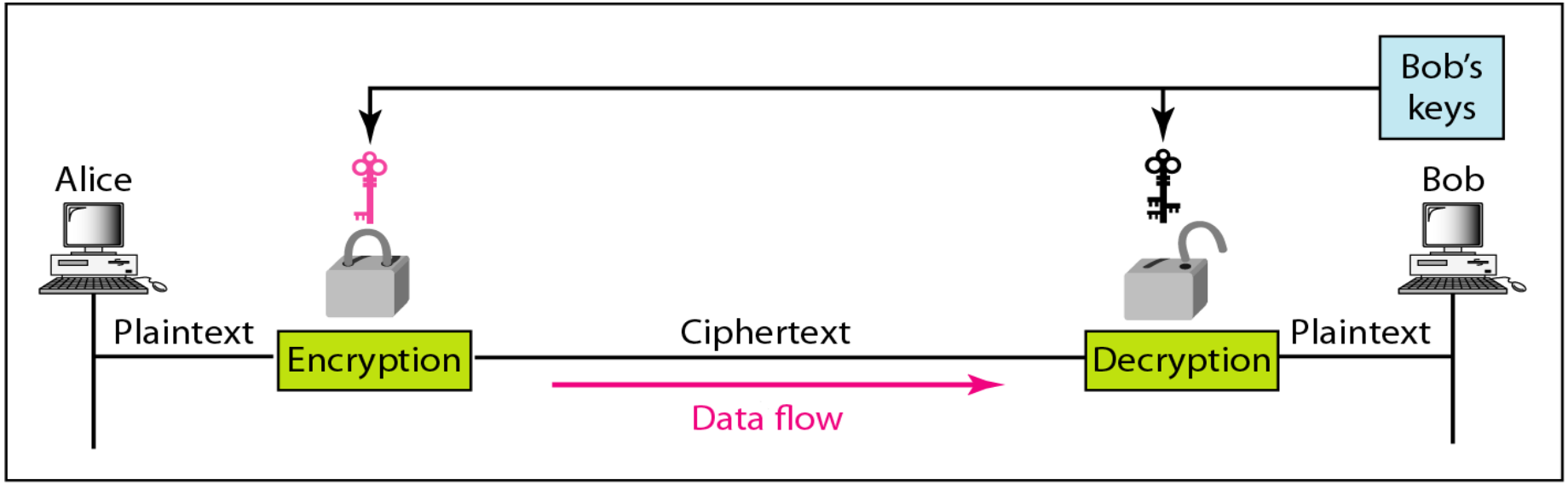
- Confidencialidade com Criptografia de Chave Simétrica
  - Chave de Sessão
  - Comunicação em ambos os sentidos
- Confidencialidade com Criptografia de Chave Assimétrica
  - Anúncio público
  - Duas chaves
    - Chave Privada
    - Chave Pública



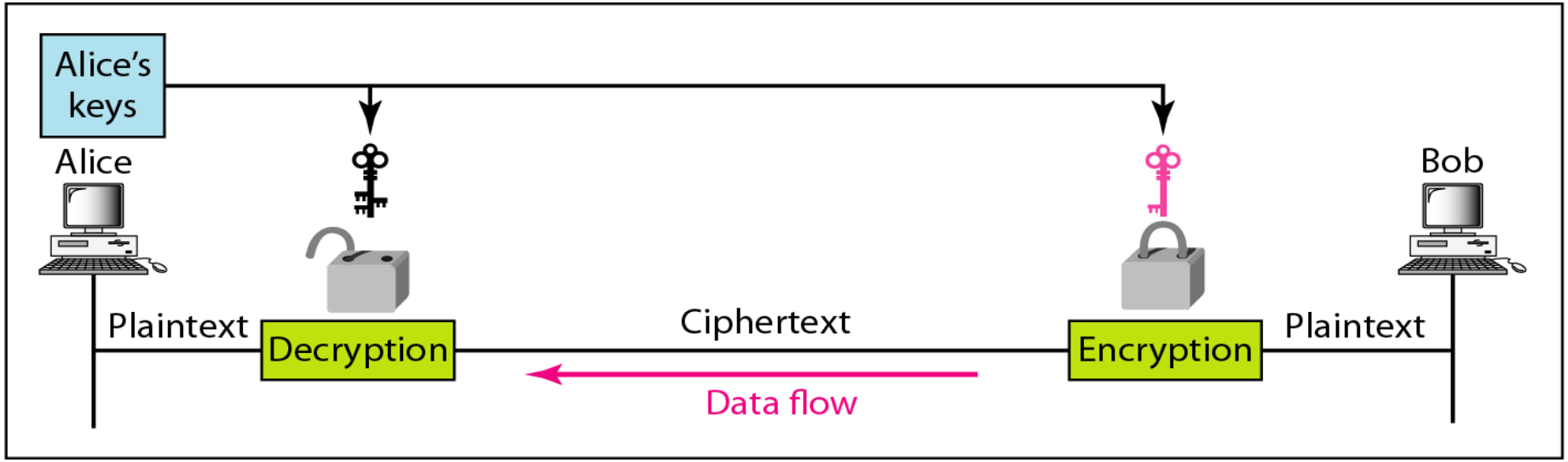
a. A shared secret key can be used in Alice-Bob communication



b. A different shared secret key is recommended in Bob-Alice communication



a. Bob's keys are used in Alice-Bob communication



b. Alice's keys are used in Bob-Alice communication

Integridade da Mensagem

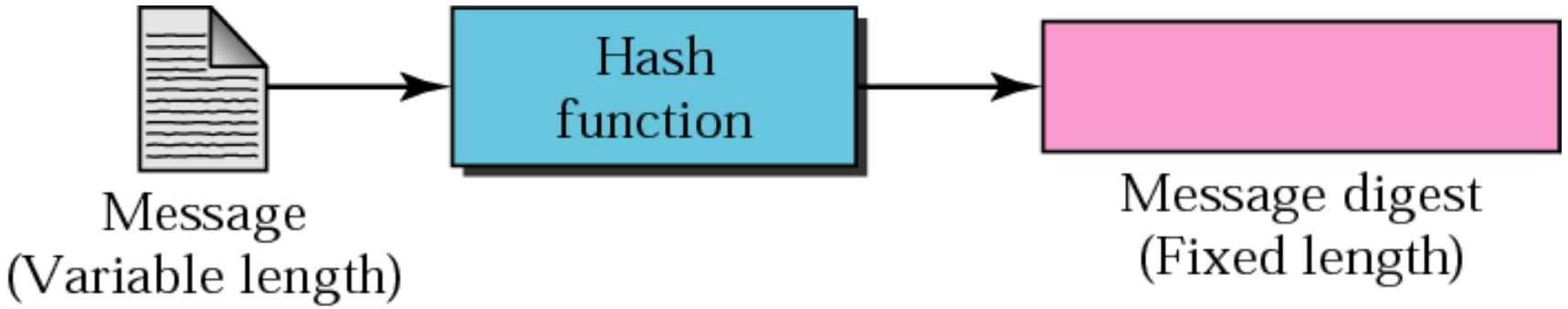
Impressão Digital:

- Certas vezes, não é necessário haver um **segredo** na troca de mensagens, e sim **integridade** (preservar, sigilo).
- Ex.: Redigir um testamento
- Função Hash/Algoritmo de Hash
  - imagem compactada da mensagem que pode ser usada como impressão digital)
  - Ex: MDC-2 (Modification Detection Code)

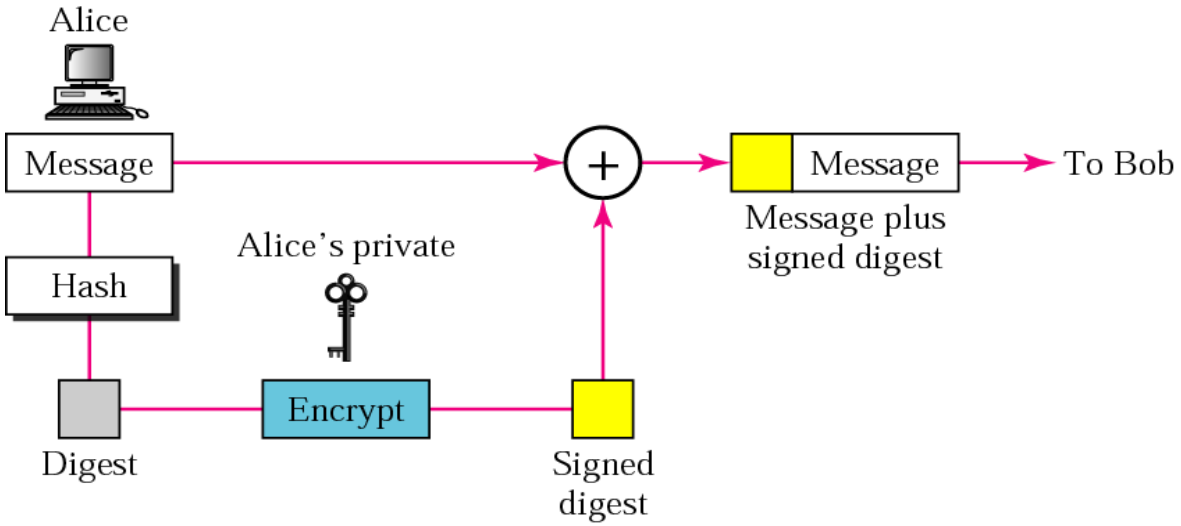
Integridade da Mensagem

Impressão Digital (2):

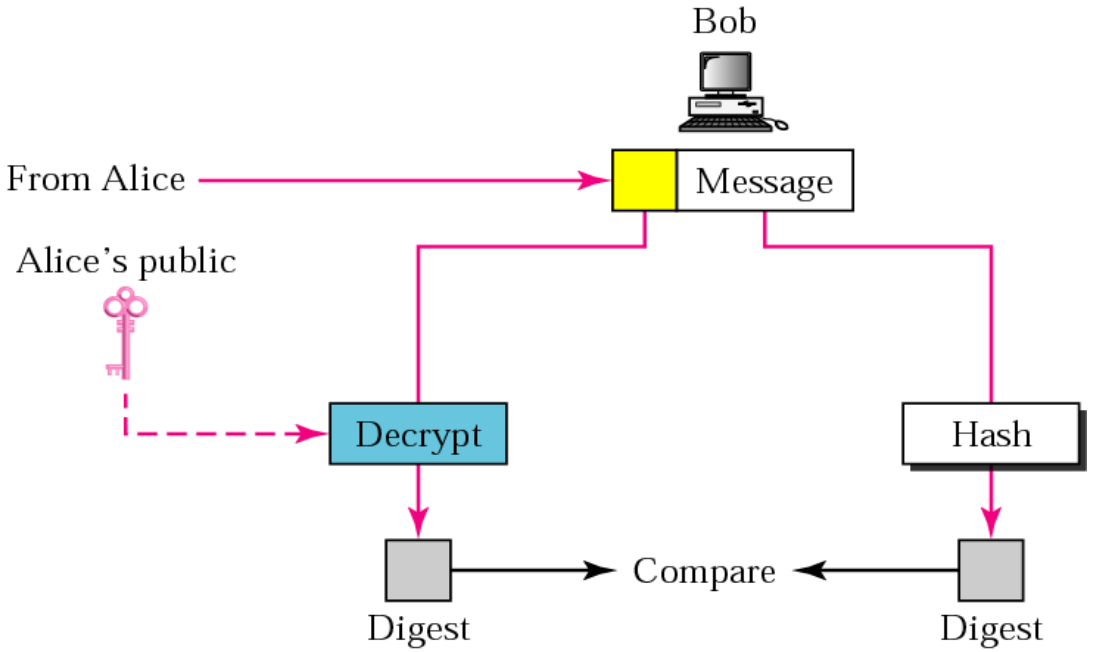
- Função Hash/Algoritmo de Hash
  - imagem compactada da mensagem que pode ser usada como impressão digital)
  - Exemplos: MD5 Message-Digest Algorithm, SHA (Secure Hash Algorithm), MDC (Modification Detection Code)



- Emissor:

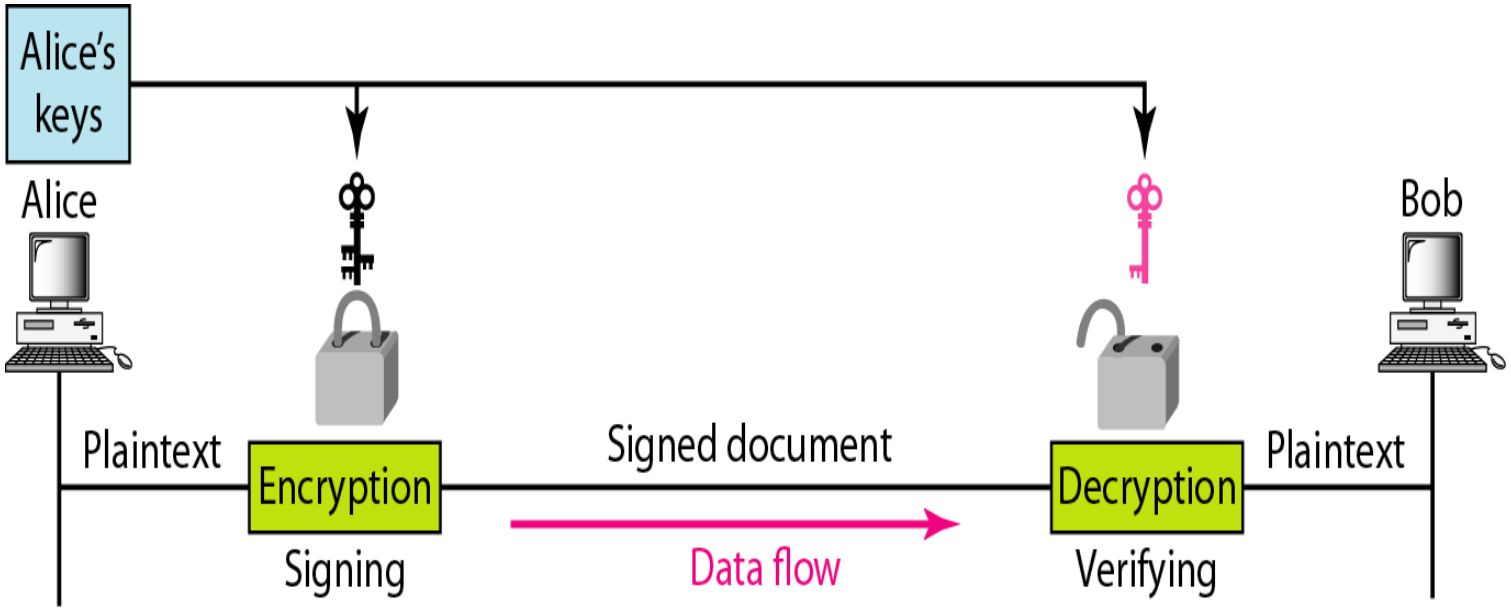


- Receptor



Assinatura Digital

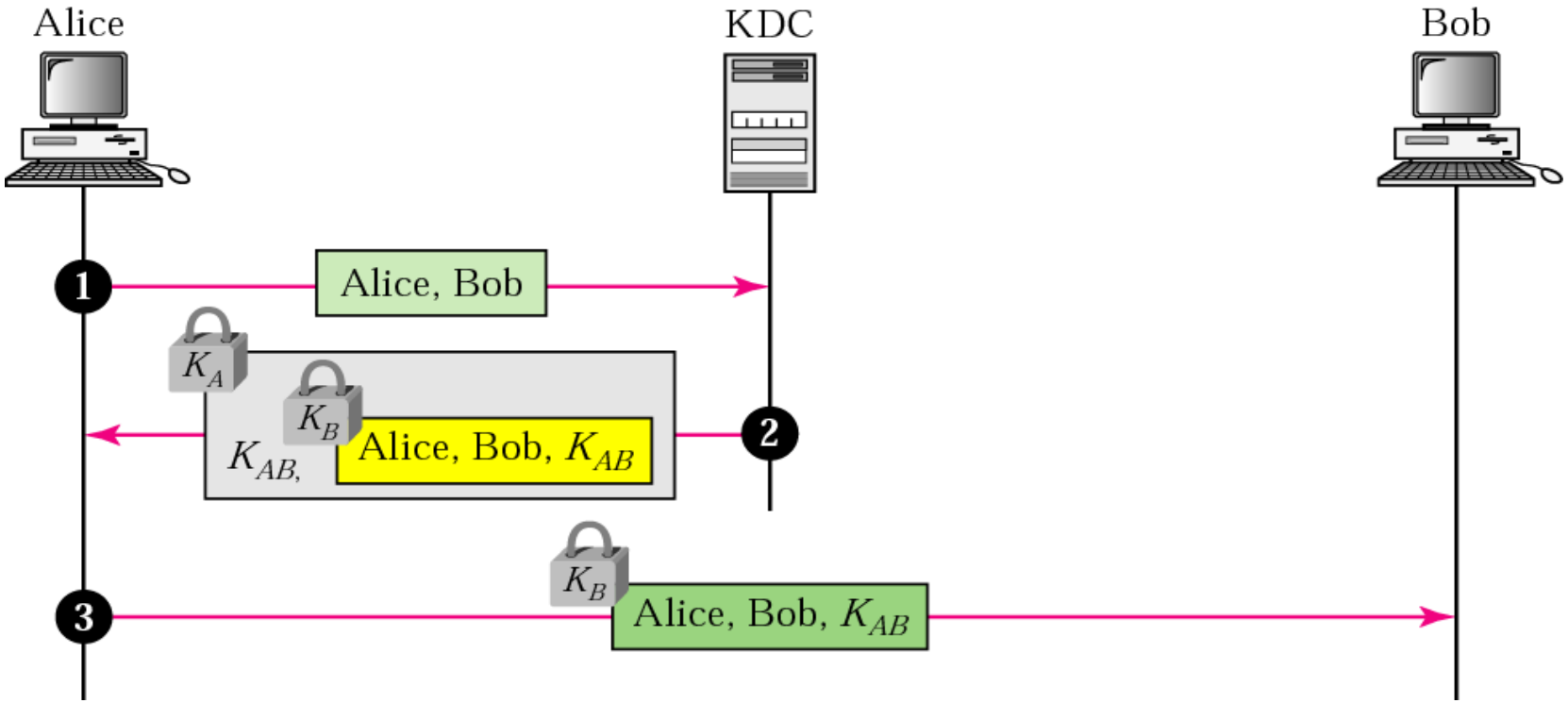
- Em um **criptossistema**, utilizamos as chaves públicas e privadas do receptor
- Na **assinatura digital**, usamos a chave pública e privada do emissor.



Autenticação de Entidades

- Entidade (pessoa, processo, cliente ou servidor)
  - Requerente e Verificador
- Diferenças entre Autenticação de Mensagens e Entidades
  - Tempo real
  - Autenticação durante toda a sessão
- Identificação Pública e Senha Privada
  - Senha Fixa
  - Senha usada apenas uma vez

Key Distribution Center (KDC)

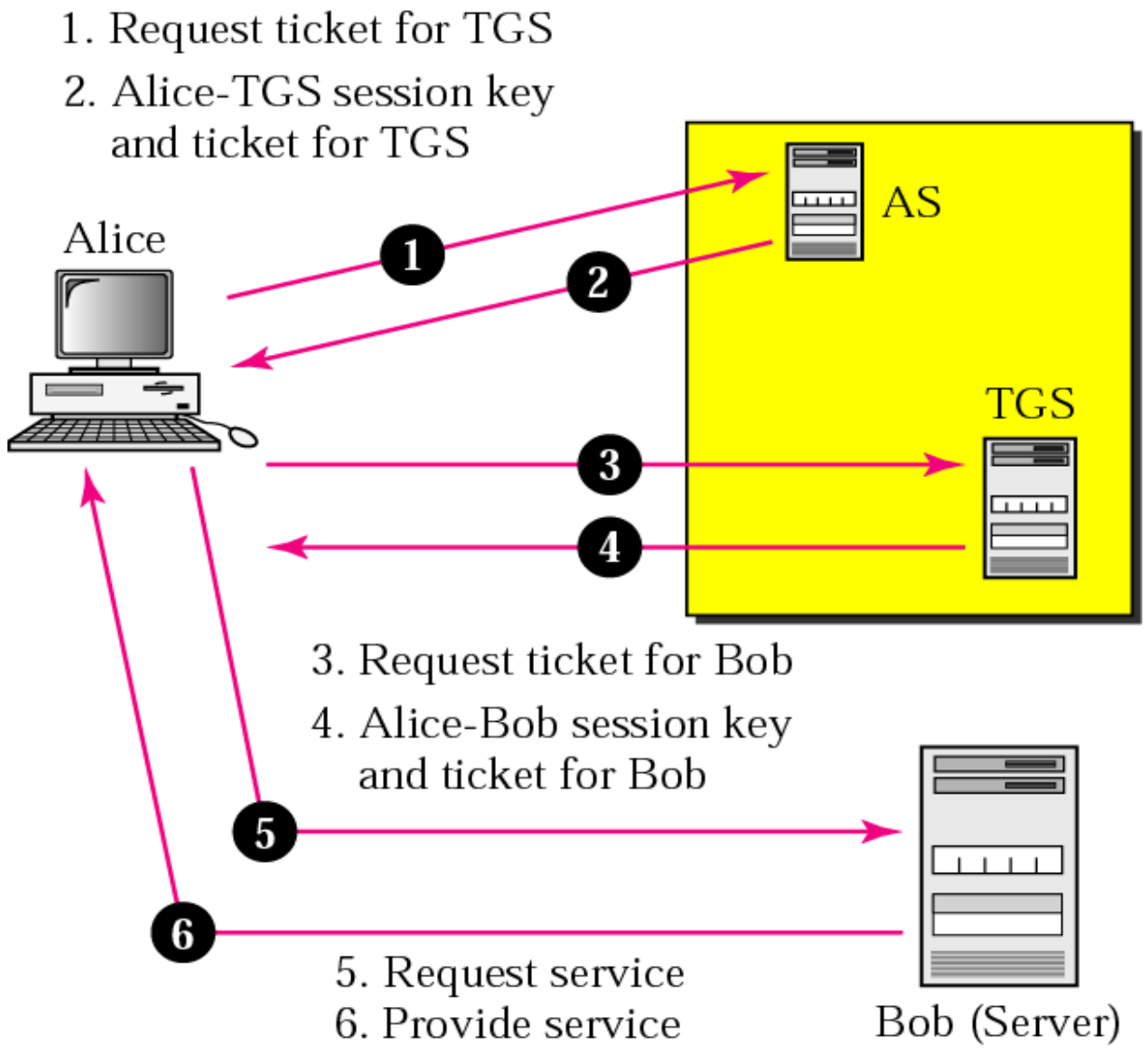


SEGURANÇA NA INTERNET

Kerberos

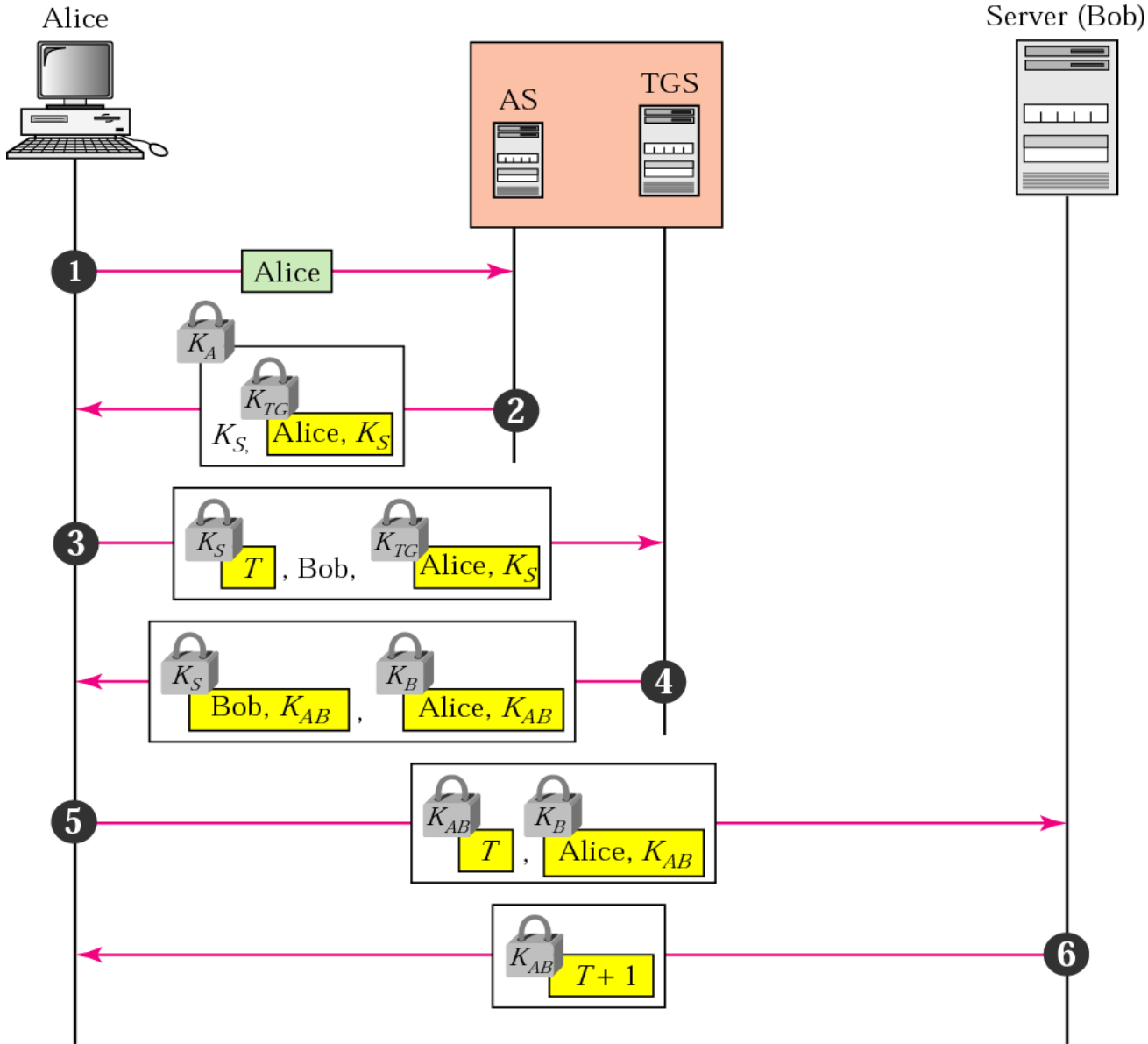
- É o KDC mais utilizado;
- Composto de duas partes:
  - Authentication Server (AS)
  - Ticket-Granting Server (TGS).

Kerberos


1. Request ticket for TGS
2. Alice-TGS session key and ticket for TGS
Alice
AS
TGS
1
2
3
4
3. Request ticket for Bob
4. Alice-Bob session key and ticket for Bob
5
6
5. Request service
6. Provide service
Bob (Server)

Kerberos

T: Ticket
K_A : Chave de Alice
K_B : Chave de Bob
K_s : Chave de sessão para o TGS
K_{TGS} : Chave do TGS
K_{AB}: Chave de sessão entre emissor e receptor



X.509

- Protocolo criado pela ITU para descrição de certificado digital;
  - Campos do X.509

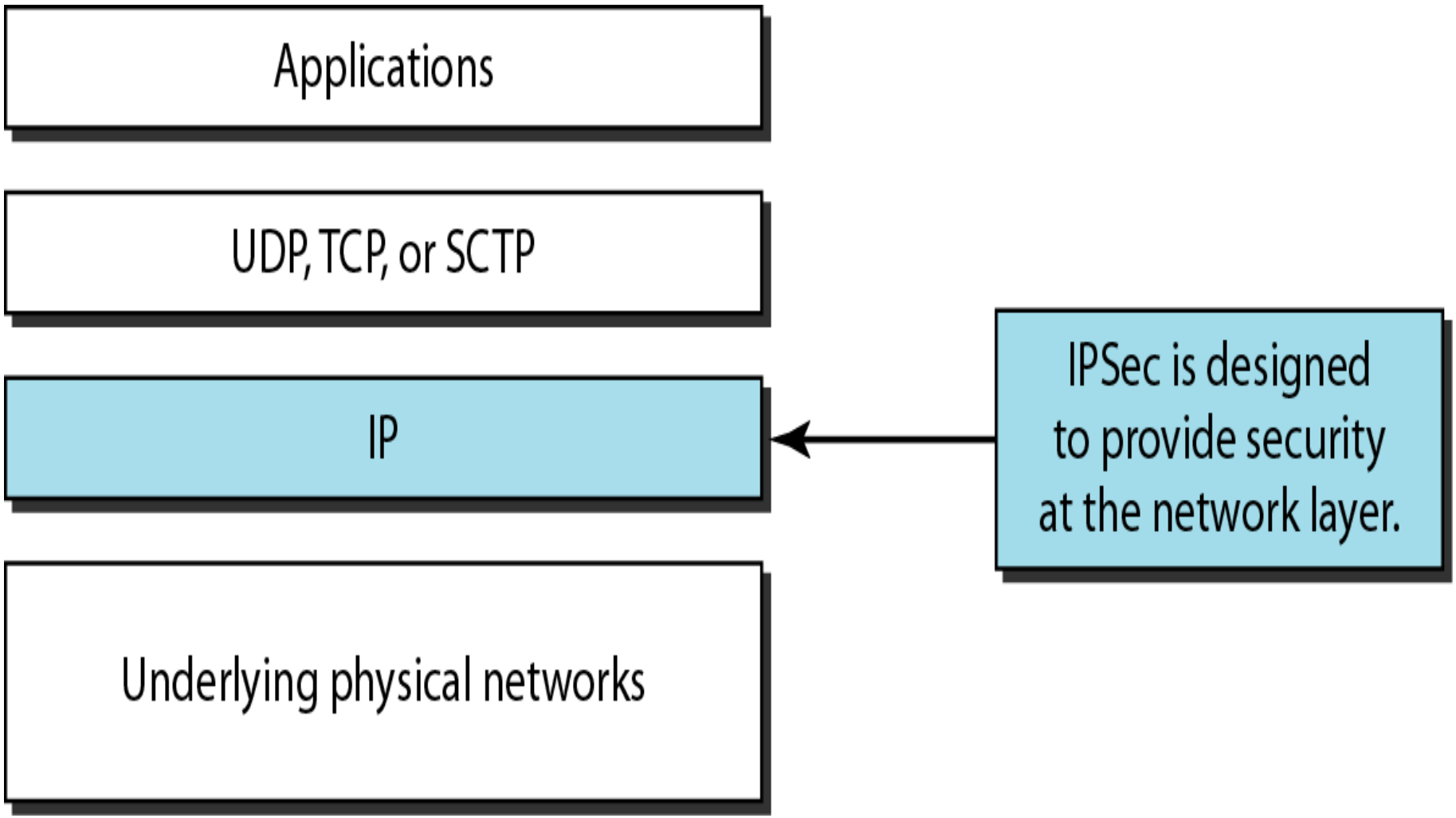
Field	*Explanation*
Version	Version number of X.509
Serial number	The unique identifier used by the CA
Signature	The certificate signature
Issuer	The name of the CA defined by X.509
Validity period	Start and end period that certificate is valid
Subject name	The entity whose public key is being certified
Public key	The subject public key and the algorithms that use it

IPSec

- É um conjunto de protocolos desenvolvido pelo IETF (Internet Engineering Task Force) para oferecer segurança para um pacote no nível de rede.
  - Pacotes confidenciais e autenticados

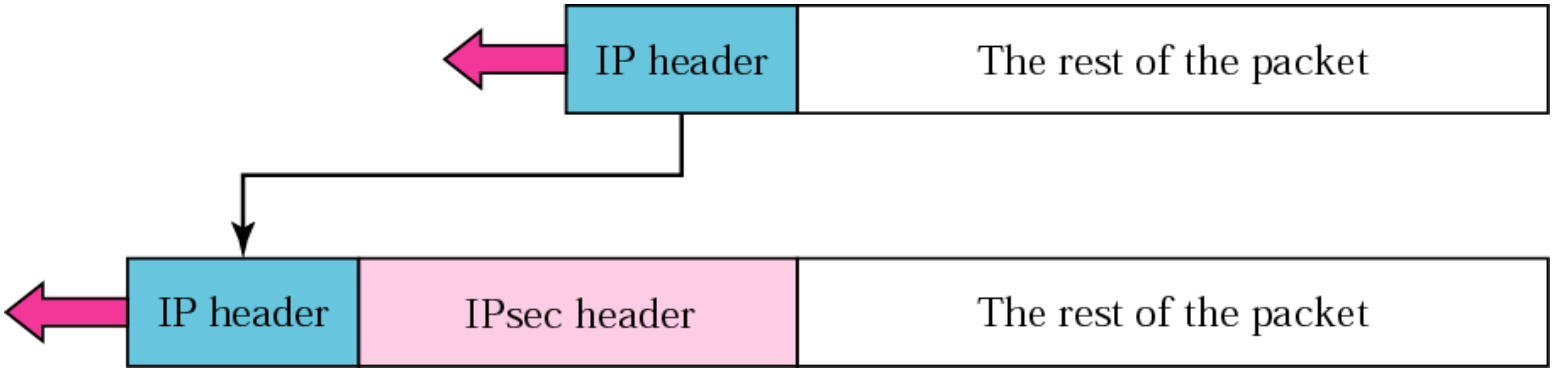
- Dois Modos
  - Modo de Transporte
  - Modo Túnel (pacote IP)

IPSec

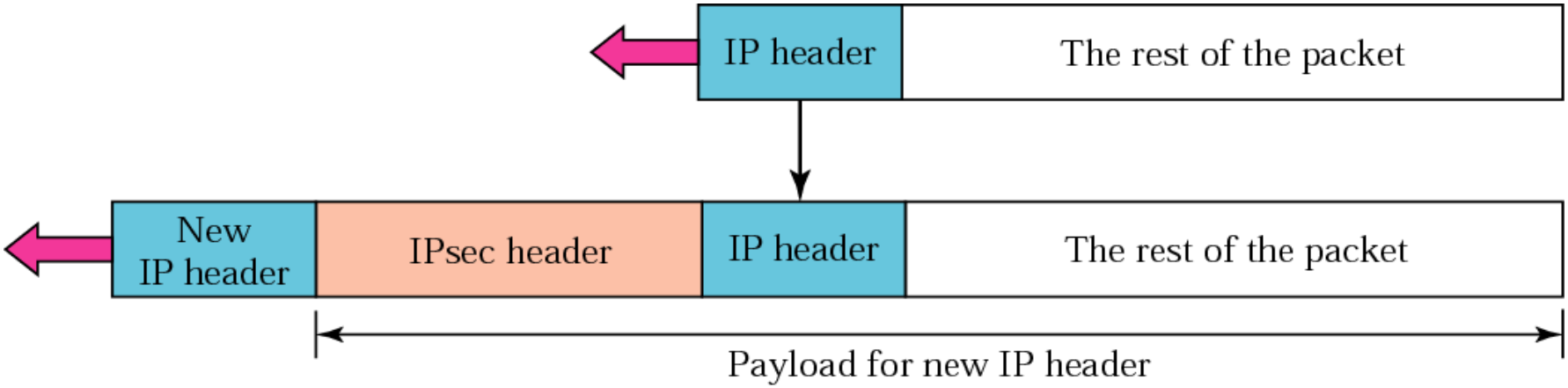

Applications
UDP, TCP, or SCTP
IP
Underlying physical networks
IPSec is designed to provide security at the network layer.

Modos do IPSec

Modo de Transporte do IPSec



Modo de Túnel do IPSec

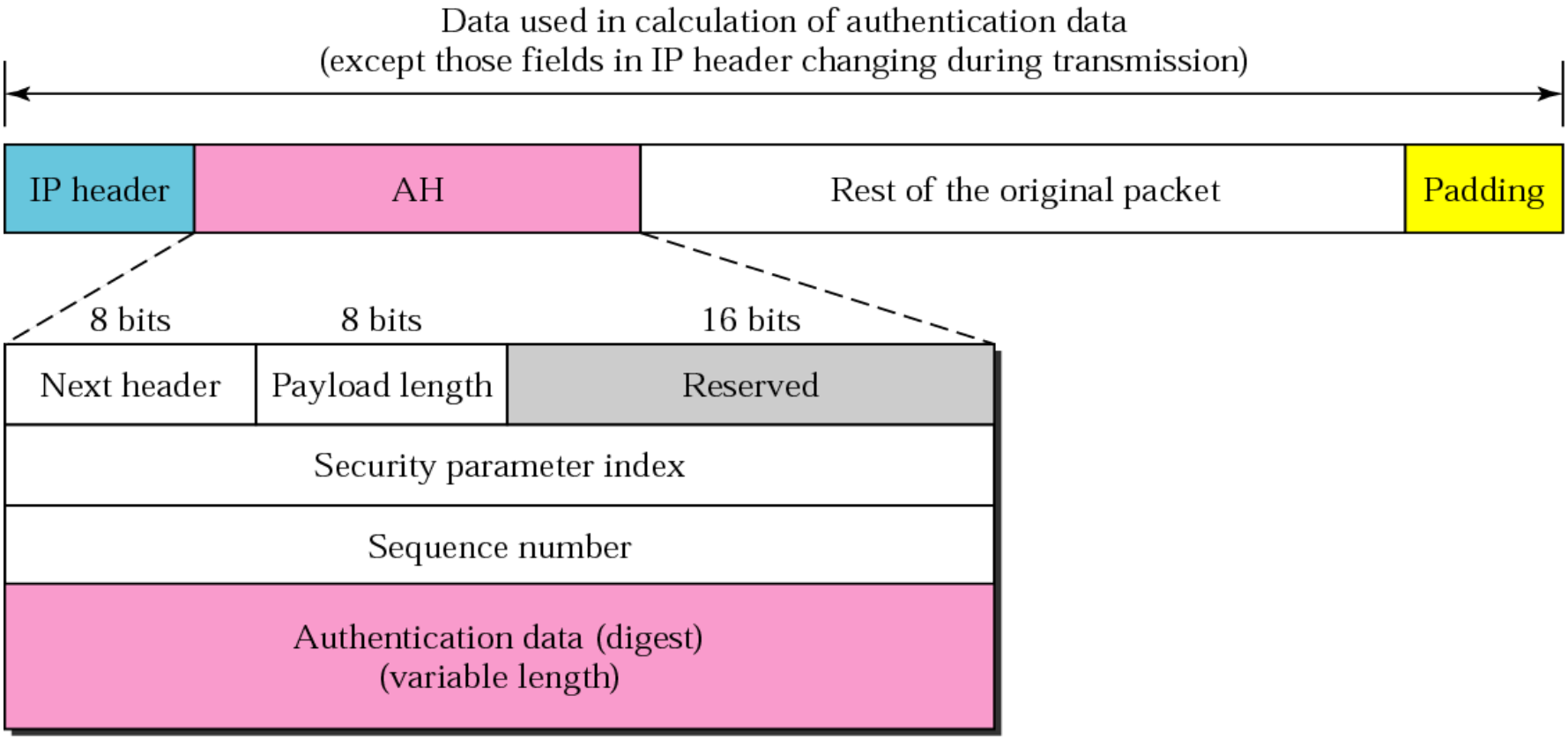


IPSec

- Dois protocolos de Segurança
  - AH (Authentication Header)
    - Fornece autenticação de fonte e integridade de dados
  - ESP (Encapsulating Security Payload)
    - Recursos de autenticação de fonte, integridade e privacidade
- Suporte ao IPv6 e IPv4

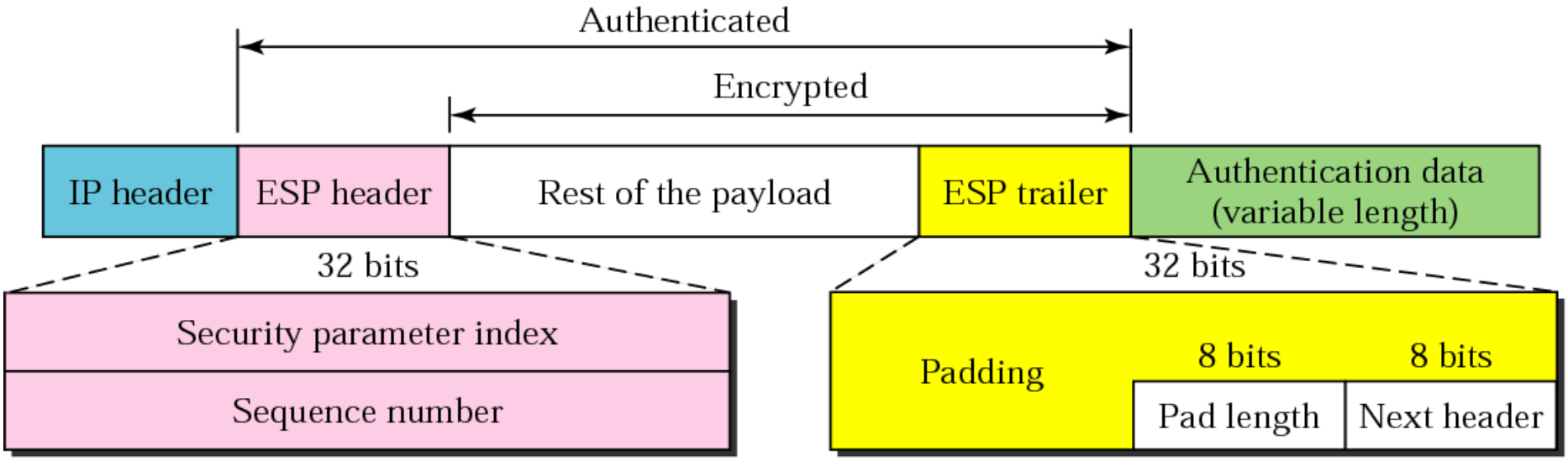
Authentication Header

- AH



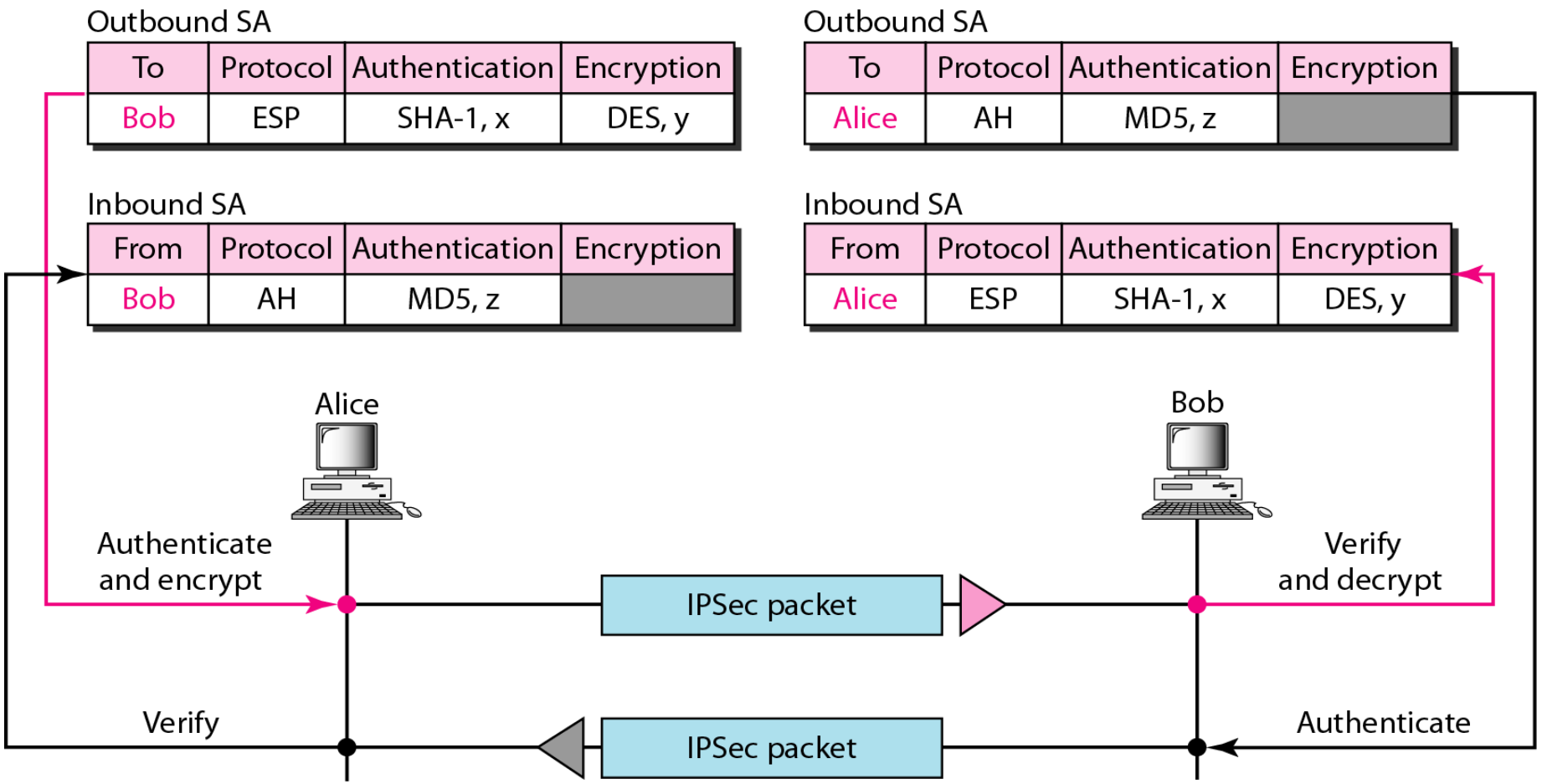
Encapsulating Security Payload

- O AH apenas permite autenticação e integridade dos dados
- O ESP é um melhoramento do AH para permitir privacidade dos dados



IPSec

- Associações de Segurança (SA – Security Association)



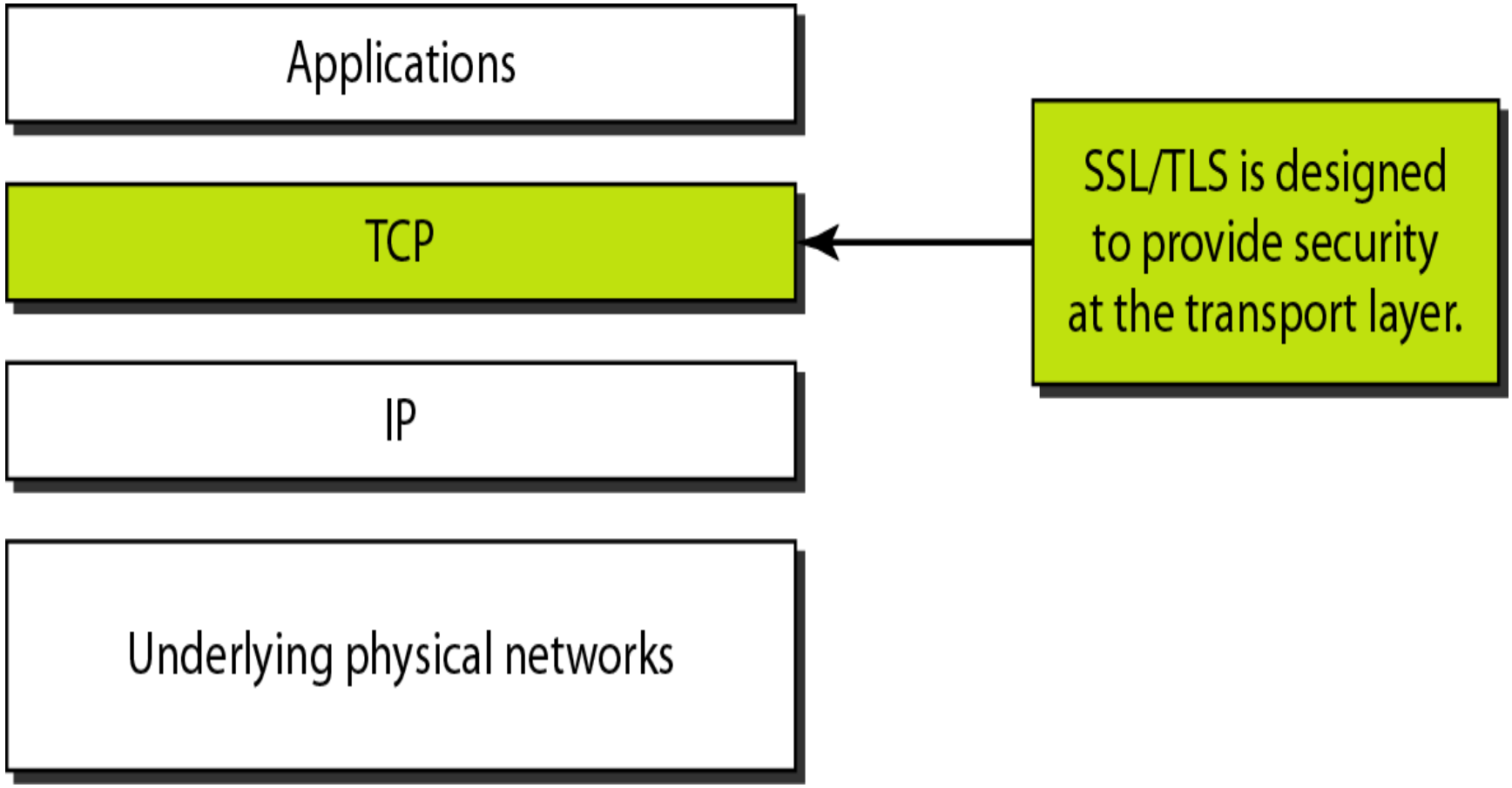
SSL/TLS

- Secure Sockets Layer
- Transport Layer Security
- Serviços de Segurança de ponta a ponta para aplicações que usam um protocolo de camada de transporte confiável, como o TCP.
  - Fornece serviços de segurança para transações na Internet.
  - Normalmente recebe serviços do HTTP

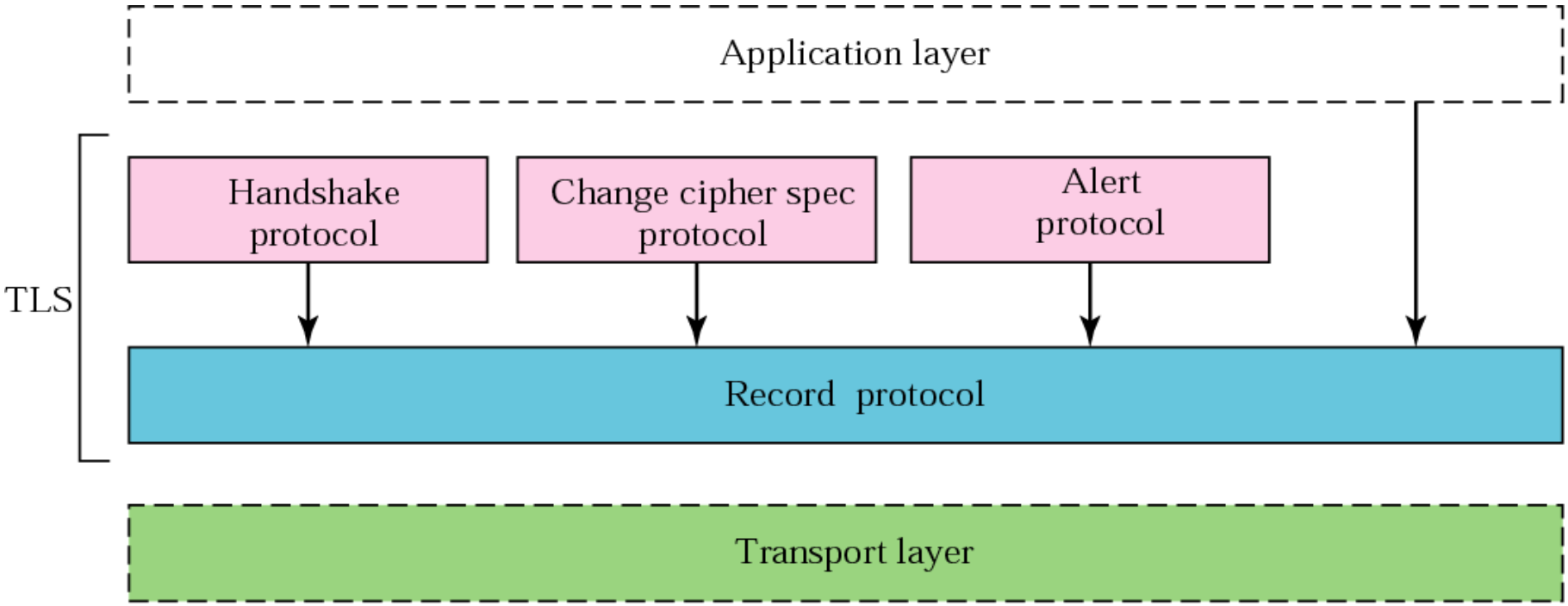
SSL/TLS

- Compras online
  - Servidor pertence ao verdadeiro fornecedor
    - Autenticação de Entidades
  - Certeza do conteúdo da mensagem
    - Integridade
  - Cliente e fornecedor precisam ter certeza deque um impostor não intercepte informações confidenciais
    - Confidencialidade

SSL/TLS

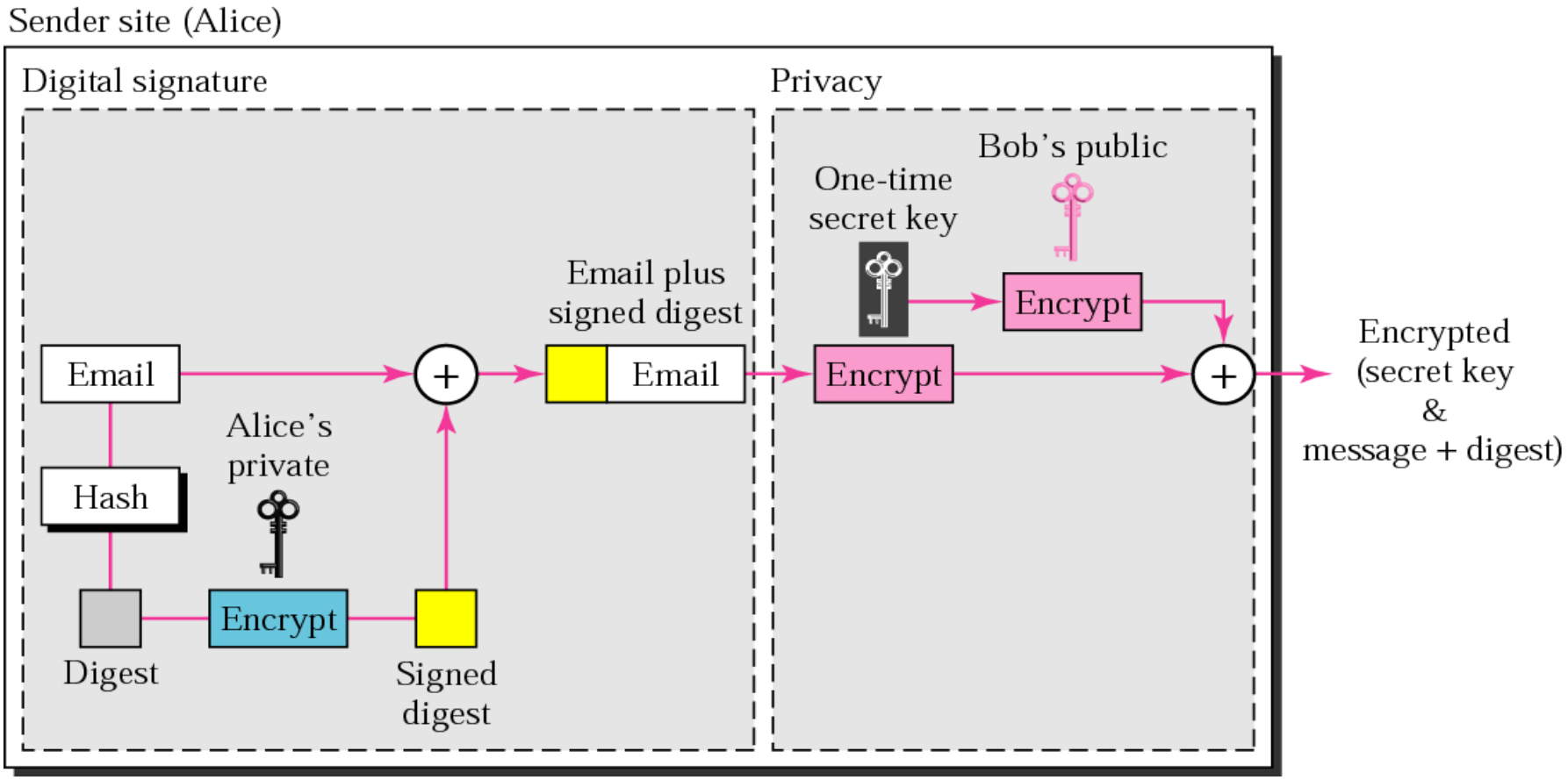

Applications
TCP
IP
Underlying physical networks
SSL/TLS is designed to provide security at the transport layer.

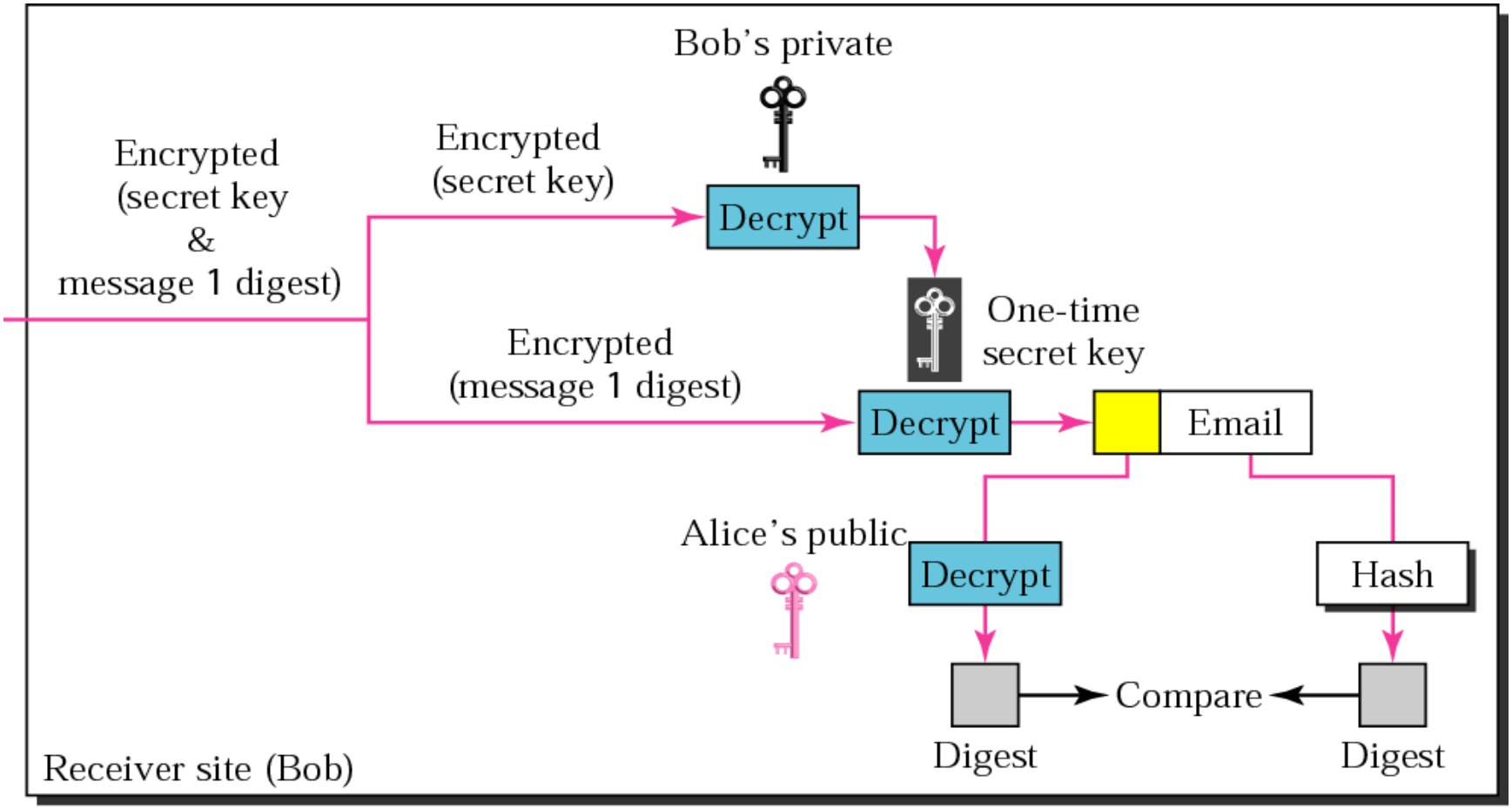
TLS


Application layer
TLS
Handshake protocol
Change cipher spec protocol
Alert protocol
Record protocol
Transport layer

Pretty Good Privacy

- O PGP foi criado para prover e-mails confidencias
  - Segurança na camada de aplicação
  - No PGP, o emissor da mensagem precisa incluir os identificadores dos algoritmos usados na mensagem, bem como dos valores das chaves.


Sender site (Alice)
Digital signature
Privacy
Email
Hash
Digest
Alice's private
Encrypt
Signed digest
Email plus signed digest
Email
One-time secret key
Bob's public
Encrypt
Encrypt
Encrypted (secret key & message + digest)

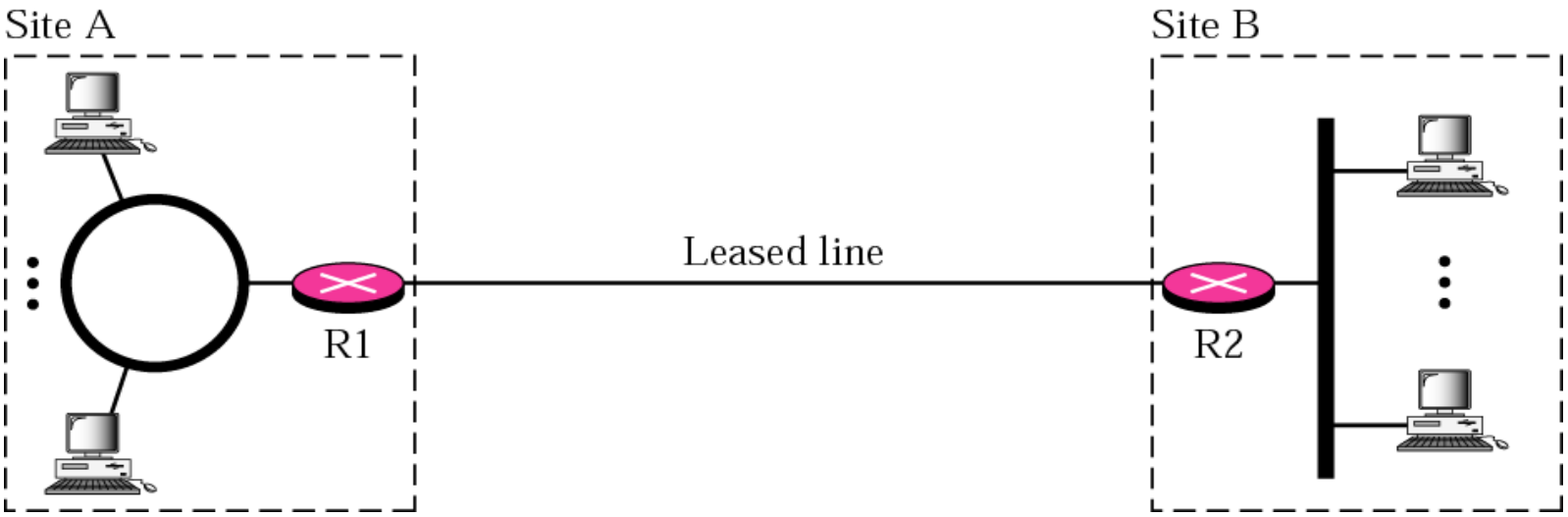

Bob's private
Encrypted
(secret key
&
message 1 digest)
Encrypted
(secret key)
Decrypt
One-time
secret key
Encrypted
(message 1 digest)
Decrypt
Email
Alice's public
Decrypt
Hash
Compare
Digest
Digest
Receiver site (Bob)

Segurança na Internet

- VPN (Virtual Private Network)
  - Aplica segurança aos datagramas IP
  - Datagrama destinado ao uso privado é encapsulado
  - Nas redes TCP/IP as VPNs são estabelecidas através do IPSec

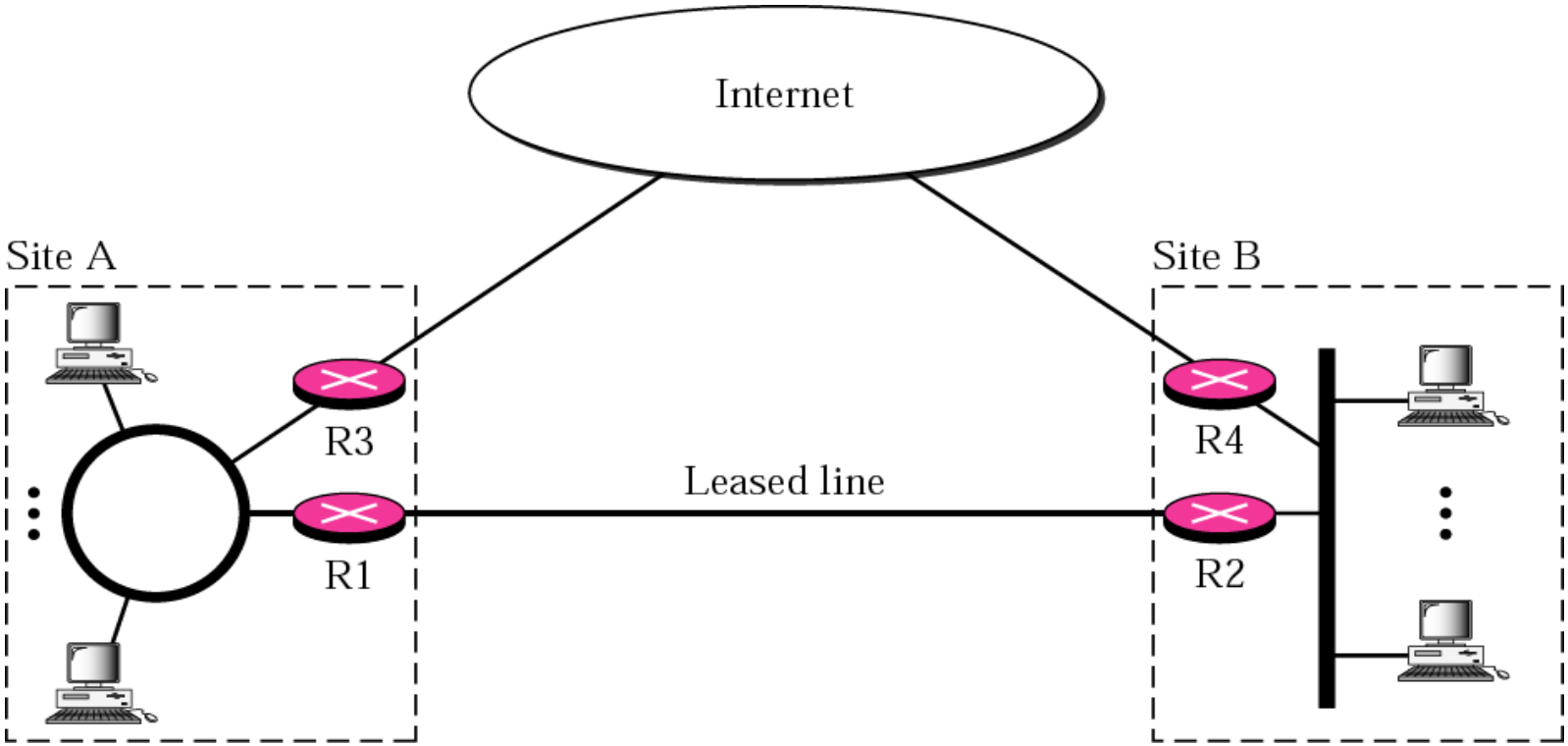
Rede Privada

- Link Privado



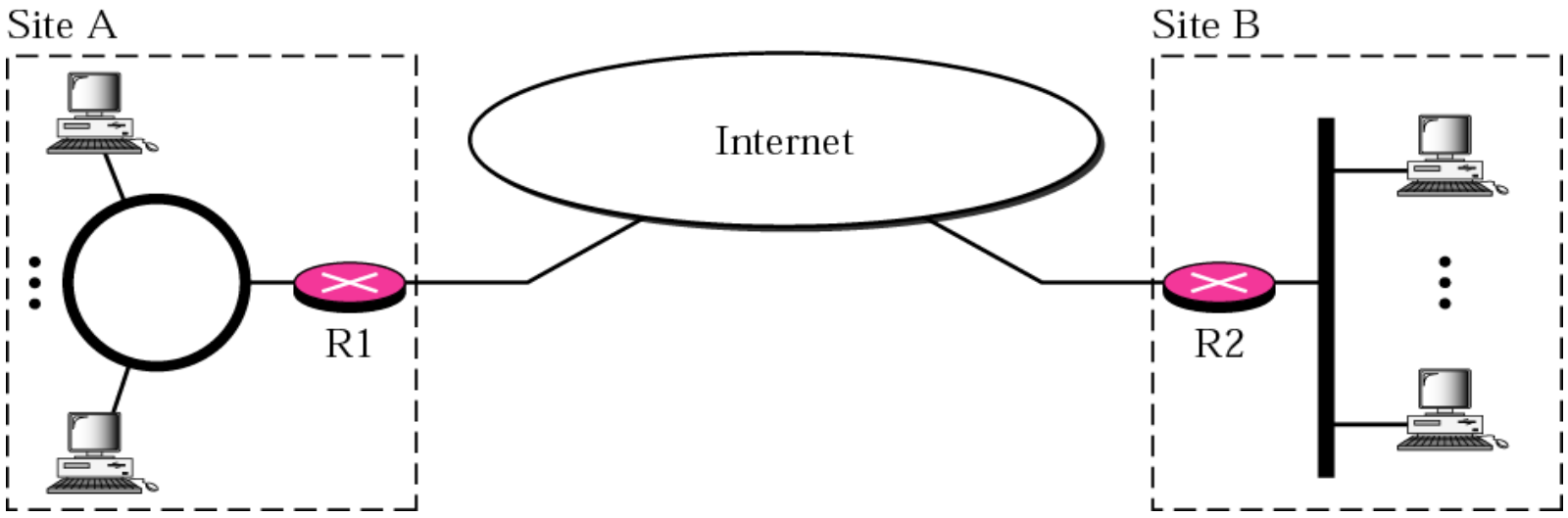
Rede Híbrida

- Links Privado e Públicos



VPN

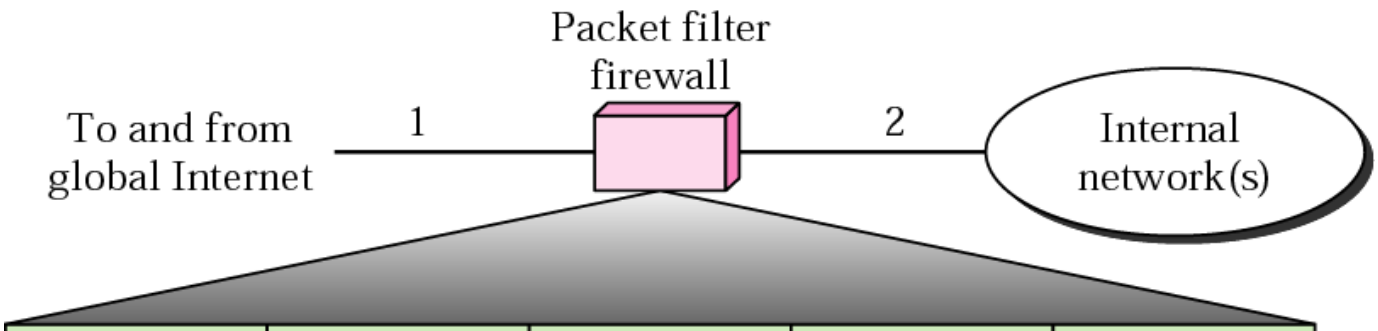
- Conexões privadas numa rede pública



Segurança na Internet

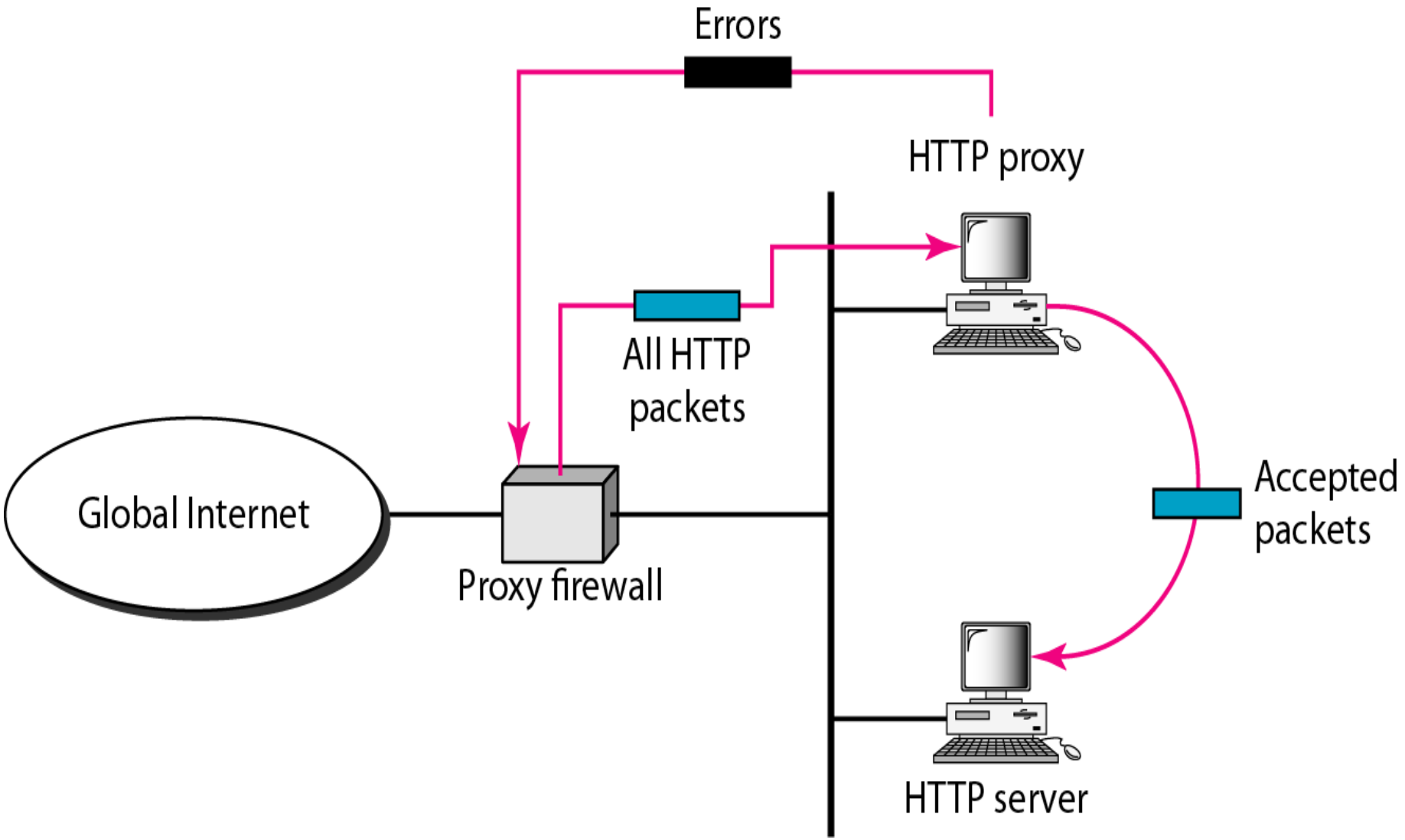
- Firewalls
- Dispositivo instalado entre uma rede interna e a Internet
- Filtragem
  - Firewall de Filtragem de Pacotes
  - Firewall de Filtragem Proxy

Packet Filter Firewall



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	*	*	80

Proxy Firewall



Outras Ferramentas para o Gerenciamento da Segurança

- IDS (Intrusion Detection System)
  - Sistema cuja função é detectar atividades incorretas, maliciosas ou anômalas.
  - Exemplo: Snort
- IPS (Intrusion Prevention System)
  - Sistema cuja função é prevenir atividades incorretas, maliciosas ou anômalas.

Outras Ferramentas para o Gerenciamento da Segurança (2)

- Scanner de vulnerabilidade
  - Utilitário que varre portas num sistema e tenta descobrir quais estão abertas e quais serviços estão disponíveis nelas.
  - Exemplos: Nmap, Nessus
- Antivírus/AntiSpyware
  - Sofware específico para prevenção, detecção e remoção de malwares (malicious software).
  - http://cartilha.cert.br/malware/

Outras Ferramentas para o Gerenciamento da Segurança (3)

- Honeypot (Pote de mel)
  - Cria hosts virtuais cuja função é mantém o invasor longe dos dados e serviços importantes;
  - Também serve como ferramenta de estudo e identificação do invasor;
  - Exemplos: Honeyd

Bibliografia

- Forouzan, Behrouz A. “Data Communications and Networking”. 4ª Edição, 2007.

- Kurose, James; Ross, Keith; “Redes de Computadores e a Internet”. Editora Pearson, 5ª Edição, 2010.

- Tanenbaum, Andrew. “Redes de Computadores”. Editora Campus, 4ª Edição, 2003.

Dúvidas?