Segurança em Redes - Parte 1

Prof. Jaime Cohen
créditos: D.Comer, D. Boneh, J.F.Kurose, K. W. Ross, R. Dahab

2025

Universidade Estadual de Ponta Grossa

Sumário

Objetivos da Segurança em Comunicação

- Sigilo/Confidencialidade
- Integridade das Mensagens
- Autenticação
- Segurança operacional

Sigilo/Confidencialidade

Sigilo/Confidencialidade

- Somente o receptor pode interpretar a mensagem
- Uso de criptografia

```
Mensagem: A aula de hoje é sobre segurança.

Mensagem Criptografada com AES/CBC + Chave + IV):

e5 1f 59 99 50 15 f4 86 1f a0 97 06 66 c8 83 3f
e4 93 4b fb 80 19 54 fc ab db 23 00 01 da e9 88
c5 59 36 21 47 06 0d 86 5a 91 a8 8c 9d 8d 78 e5
```

Autenticação

Autenticação

- certificar a identidade da outra ponta
  - cliente autentica a identidade do servidor
  - cada ponta autentica a outra
- autenticação de mensagens
  - correio eletrônico, registros de DNS (DNSSEC), roteadores

Integridade de Mensagens

- impede que as mensagens não sejam alteradas sem detecção

Ameaças na Comunicação

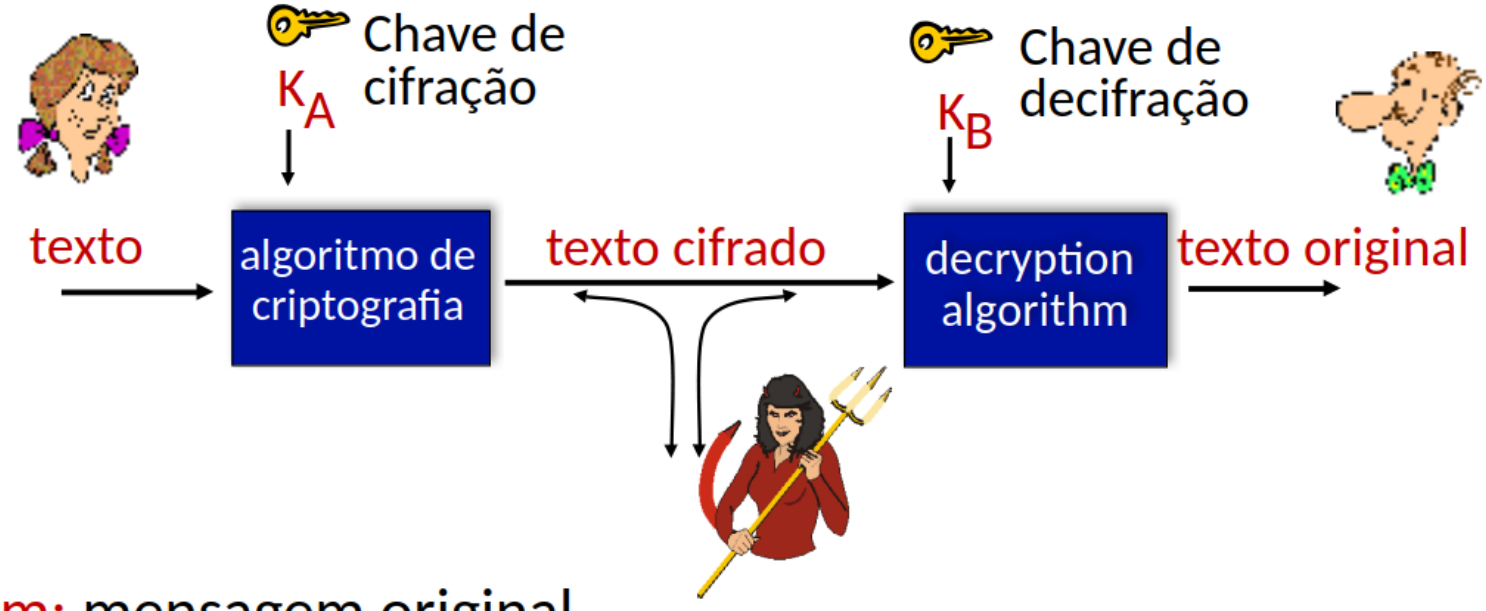
Ameaças na Comunicação

- interceptar mensagens
- inserir mensagens nas conexões
- falsificação de identidade
- roubo de sessão
- negação de serviço

Criptografia

A criptografia é o processo de codificar informações para protegê-las contra acesso e modificação não autorizados, de forma que apenas as partes autorizadas com a chave apropriada possam acessar e verificar sua integridade.

Criptografia



m: mensagem original

$K_A(m)$: texto cifrado com a chave K_A

$m = K_B(K_A(m))$

Ataque à Criptografia

Ataque à Criptografia

- ataque ao texto cifrado
  - força bruta
  - análise estatística
- com não cifrado conhecido
  - tem exemplos de encriptação
- texto não cifrado escolhido
  - pode escolher exemplos para serem encriptados

Criptografia

- Algoritmos conhecidos
- Chaves
- Criptografia Simétrica
  - Rápida
  - Segura
- Criptografia Assimétrica
  - Permite a troca de chaves
  - Usada na Autenticação (pessoas, sites, servidores)
  - Assinatura Digital
  - Certificado Digital
  - Autoridade Certificadora

Integridade das Mensagens

- Alterações nas Mensagens são detectadas
  - erros
  - alterações maliciosas

Universidade Estadual de Ponta Grossa

Autenticação

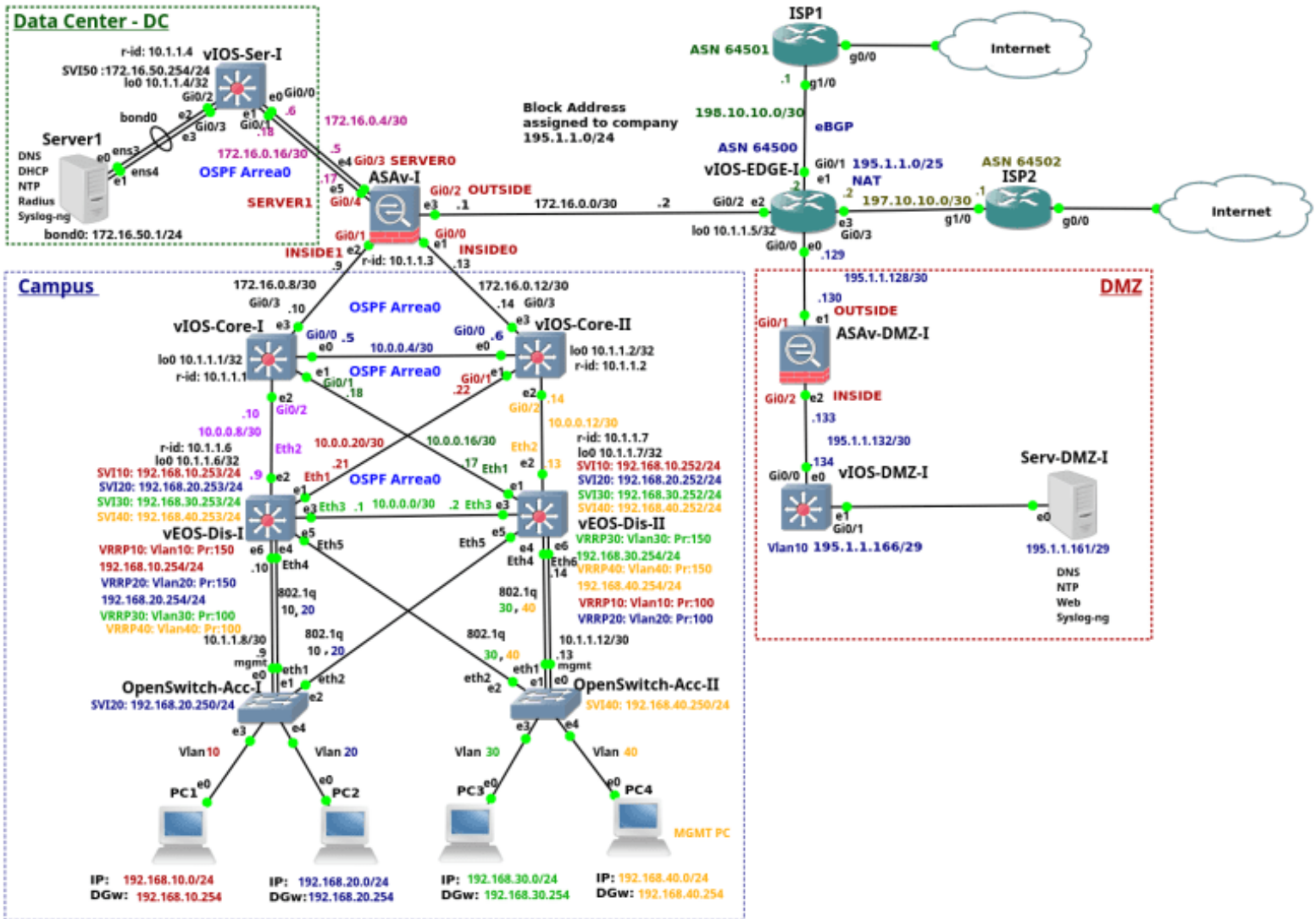
- Autenticação de Usuários
  - protocolo de autenticação
  - autorizações
- Autenticação de Computadores e Sistemas
- Autenticação de Mensagens

Segurança Operacional

- Firewalls
- Sistemas de Detecção/Prevenção de Intrusos
- Proteção da Infraestrutura
- DNSSEC, IPsec, VPNs, TLS, ssh

Topologia de Redes e Firewalls

Exemplo:



Universidade Estadual de Ponta Grossa

Tipos de Comprometimento de Segurança na Rede

- Roubo de dados
- Negação de serviços
- Controle de máquina remota
- *Phishing* / Estelionato

Técnicas de Ataque

- Interceptação de dados
- Modificação, inserção e repetição de mensagens
- Exploração de bugs em software como estouro de buffer
- *Spoofing*: de endereço físico, endereço IP, endereço de e-mail
- Ataques de negação de serviço
  - Inundação de pacotes SYN (TCP)
- Descoberta de chaves ou senhas
- Varredura de portas

Técnicas Usadas na Segurança de Redes

- *Hashing*
- Criptografia
- Assinaturas digitais
- Certificados digitais
- *Firewall*
- Sistemas de detecção de intrusos
- Sistemas de análise de pacotes e conteúdo
- Redes Privadas Virtuais (VPNs)

Usos da Criptografia

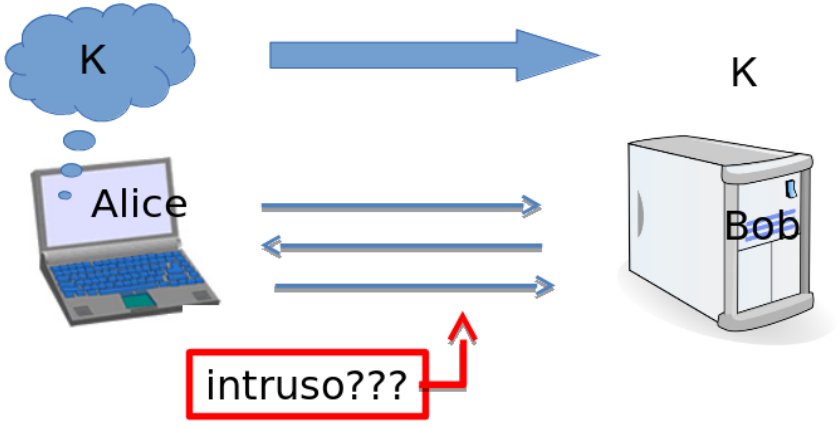
- Comunicação segura: HTTPS, WPA, GSM, Bluetooth
- Criptografia de arquivos: encfs, TrueCrypt
- Proteção de conteúdo (DVD, Blue-ray): DRM (*Digital Rights Management*) (CSS, AACS)
- Autenticação

Usos de Criptografia: SSL/TLS - Secure Socket Layer

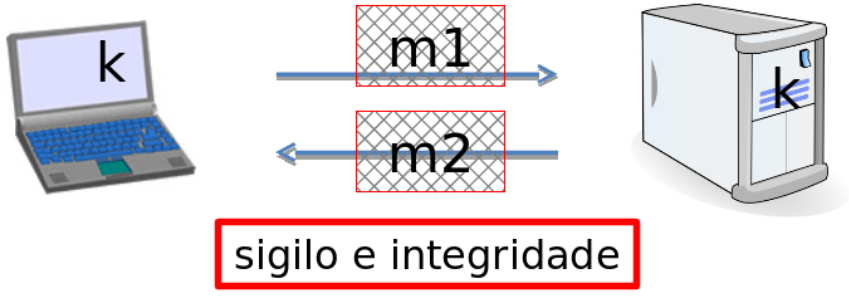
1. Protocolo de Conexão:
   - negociação de métodos criptográficos
   - compartilhamento de uma chave secreta
2. Autenticação com certificados digitais
3. Transmissão de Dados: usando a chave compartilhada na criptografia
4. Confidencialidade e Integridade

Usos de Criptografia: SSL/TLS - Secure Socket Layer

Compartilhamento de chave:



Comunicação segura:



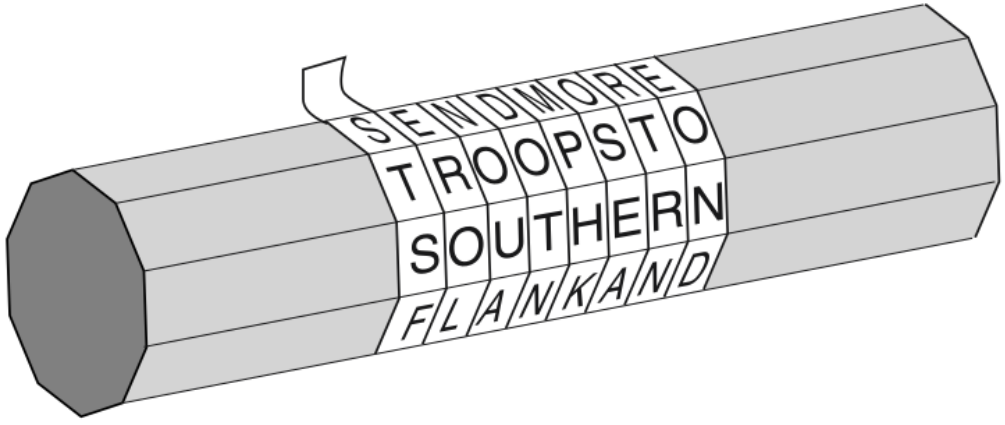
Universidade Estadual de Ponta Grossa

Antes do Século 20

- Vários relatos de uso na antiguidade:
  - Grécia antiga, Império Romano, Índia, Árabes, etc.
- Estenografia
- Criptografia
  - transposição
  - substituição

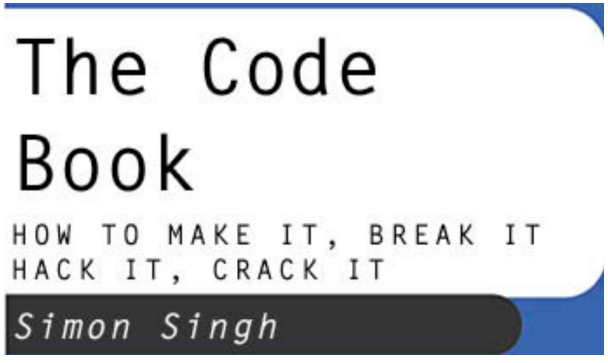
Antes do Século 20

Scytale, séc.V A.C.



Antes do Século 20

Livro sobre história da criptografia e curiosidades:



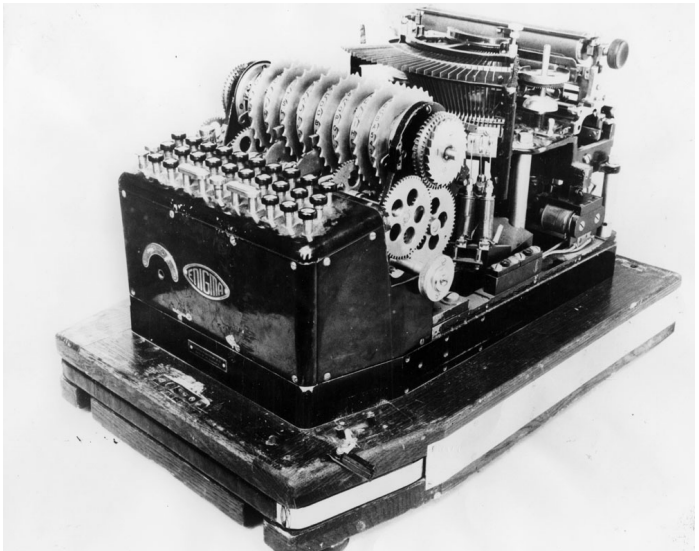
Universidade Estadual de Ponta Grossa

História - Século XX

- Enigma
- Bletchley Park (Government Code and Cypher School)
- Alan Turing
- Colossus (Prim. Comp. Digital Programável)

Universidade Estadual de Ponta Grossa

História - Segunda Guerra Mundial



História - Segunda Guerra Mundial

Historia - Criptografia de Chave Pública

- James H. Ellis, Clifford Cocks, and Malcolm Williamson at the Government Communications Headquarters (GCHQ) in the UK, 1973 (divulgado em 1997)
- W. Diffie, M. Hellman, R. Merkle, 1976
- Ron Rivest, Adi Shamir and Leonard Adleman (RSA) - 1977

Criptografia e Criptoanálise

Criptologia - Classificação

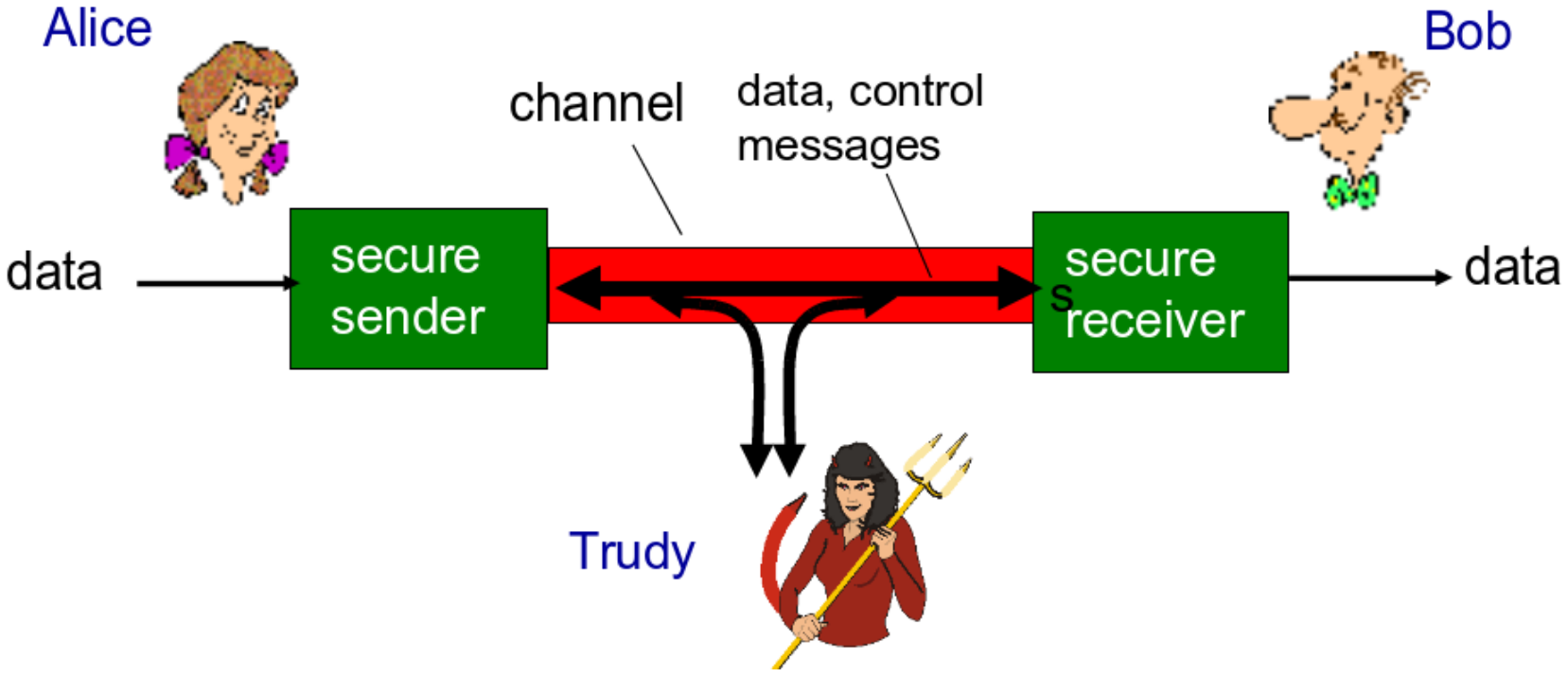
- Criptoanálise
- Criptografia
  - Cifras Simétricas
    - Cifras de blocos
    - Cifras de fluxo
  - Cifras Assimétricas
  - Protocolos

Criptografia - Conceitos Importantes

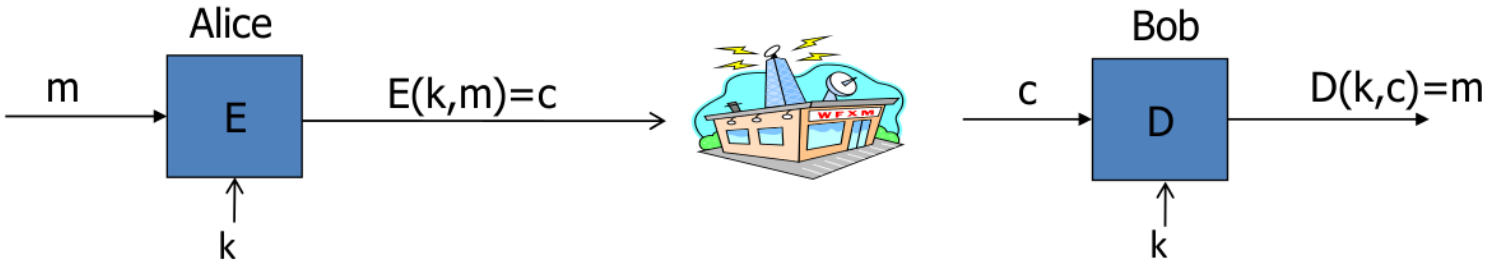
O principais conceitos utilizados pelos métodos criptográficos são:

- Funções e permutações pseudoaleatórias
- Funções de Espalhamento (*hash*)
- OU Exclusivo (XOR $\oplus$)
- Números Primos e Fatoração (criptografia de chave pública)

Criptografia



Criptografia

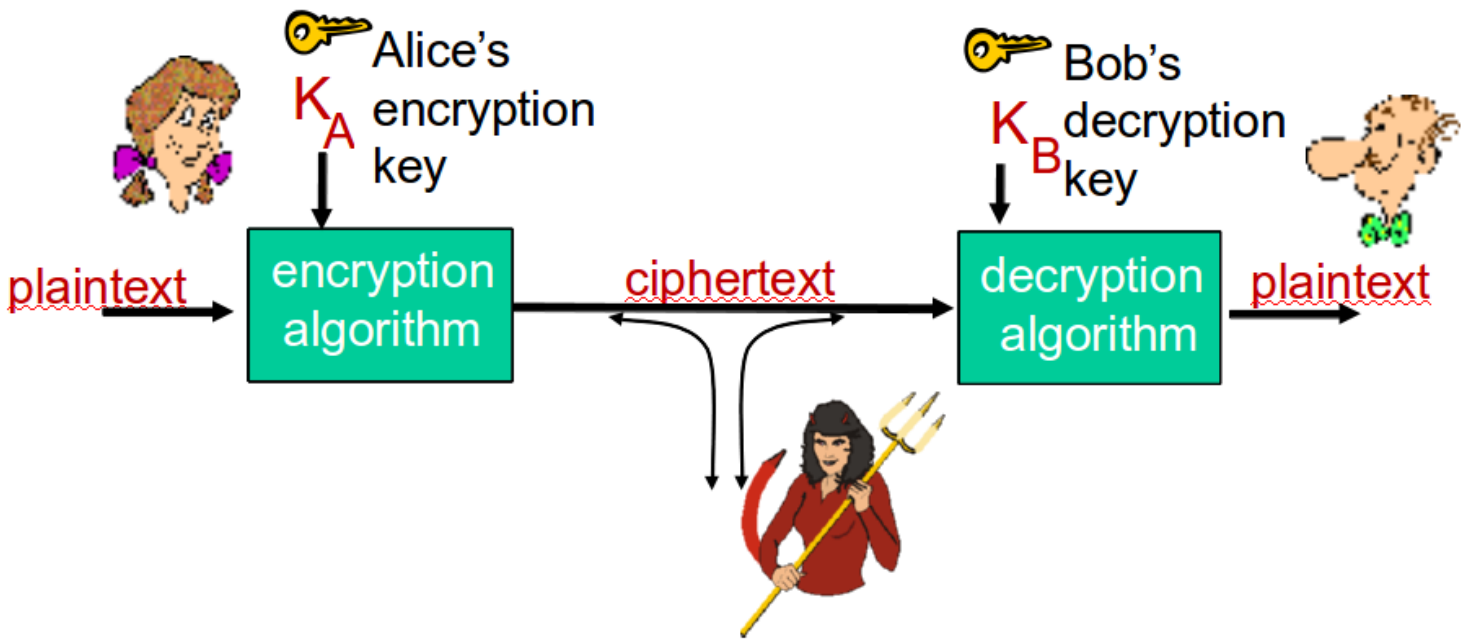


- E(), D() : algoritmos para criptografar, decriptografar
- k : chave secreta/privada (e.g. 128 bits)
- Algoritmos são públicos

Criptografia - Chaves

- Chaves podem ser usadas uma única vez
- Chaves podem ser usadas múltiplas vezes

Criptografia



Universidade Estadual de Ponta Grossa

Criptoanálise

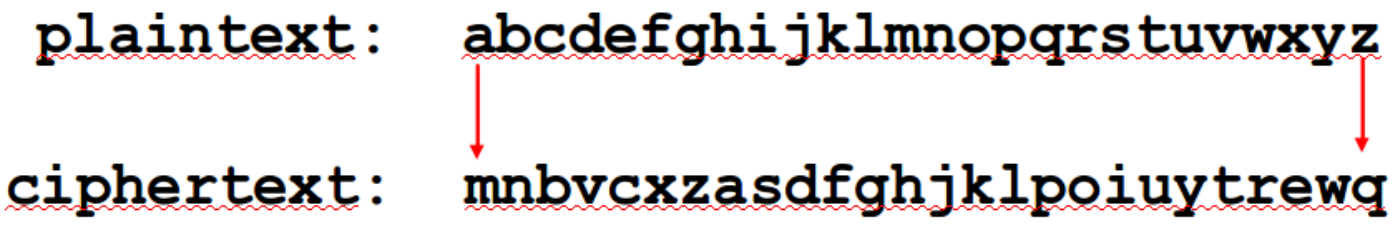
- Baseado no texto cifrado
- Com texto cifrado + mensagem
- Mensagem escolhida + texto cifrado

Universidade Estadual de Ponta Grossa

Criptografia de Chave Compartilhada

- Métodos monoalfabéticos, polialfabéticos (histórico)
- DES, 3DES, AES - modos CBC

Criptografia de César



e.g.: Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc

Criptografia de César

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Criptografia de Vigener

k	=	C	R	Y	P	T	O	C	R	Y	P	T	O	C	R	Y	P	T
m	=	W	H	A	T	A	N	I	C	E	D	A	Y	T	O	D	A	Y
c	=	Z	Z	Z	J	U	C	L	U	D	T	U	N	W	G	C	Q	S

(+ mod 26)

Criptografia Assimétrica

- Não é necessário o compartilhamento de chaves secretas
- Cada usuário gera o seu próprio par de chaves
- Se n agentes querem se comunicar, $2n$ chaves são suficientes
- Na criptografia simétrica, $\binom{n}{2} = \frac{n \times (n-1)}{2}$ chaves são necessárias

Criptografia Assimétrica

- Cocks (1973 - segredo militar até 1997)
- Diffie-Hellman (1976)
- RSA - Rivest-Shamir-Adleman (1978)

Conceitos Básicos: Ou Exclusivo

O OU exclusivo (XOR) de duas sequências de bits é a soma bit a bit módulo 2.

- Exemplo:

$$0011 \oplus 0101 =$$

Conceitos Básicos: Ou Exclusivo

Uma propriedade importante do ou exclusivo é:

- Seja $X = \{0,1\}^n$. Seja $Y = \{0,1\}^n$ uma sequência aleatória, uniformemente distribuída e independente.

Então: $Z = X \oplus Y$ é uma sequência aleatória uniformemente distribuída.

Notação: $\{0,1\}^n$ é uma sequência binária de comprimento n.

Método Criptográfico

Uma método criptográfico é uma par de funções (E, D) computáveis eficientemente tal que
$E : K \times M \rightarrow C$,

$D : K \times C \rightarrow M$

onde M é o espaço das mensagens de texto aberto, C é o espaço das mensagens criptografadas, e K é o espaço das chaves secretas e compartilhadas.

E, Criptografa
D, Descriptografa

One-time Pad (OTP), Vernam (1917)

One-time pad (OTP)

- A mensagem $M = \{0,1\}^n$
- A chave $K = \{0,1\}^n$
- $C = E(K, M) = K \oplus M$
- $D(K, C) = C \oplus K$

- Método seguro, pouco prático

Chaves Pseudoaleatórias

Gerador pseudoaleatório:

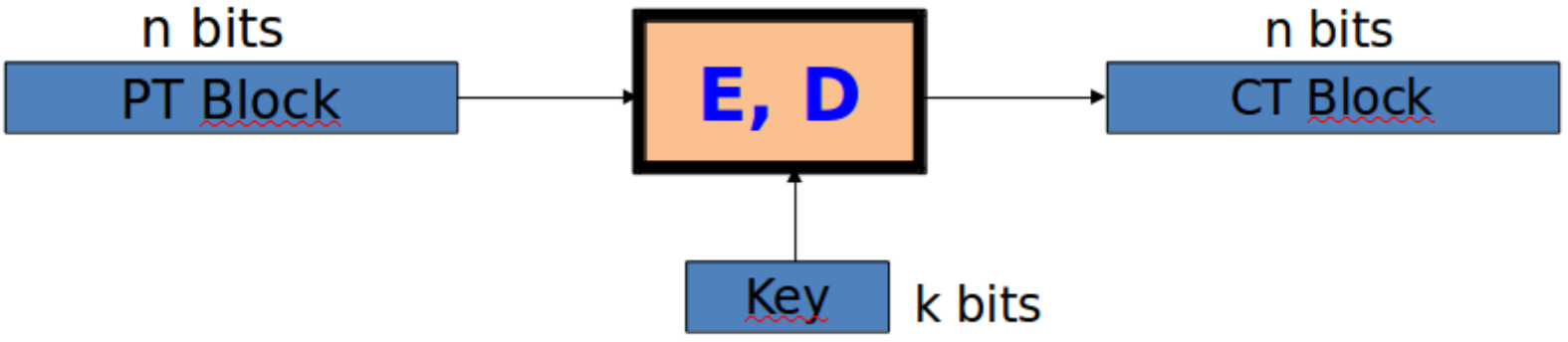
$G : \{0,1\}^s \rightarrow \{0,1\}^n$ para n bem maior do que s

Criptografia de Fluxo (*stream cipher*)

Exemplos:

- RC4, CSS, A5, LFSR (fracos)
- Salsa20
- Chacha20

Criptografia de Blocos - 1 Bloco

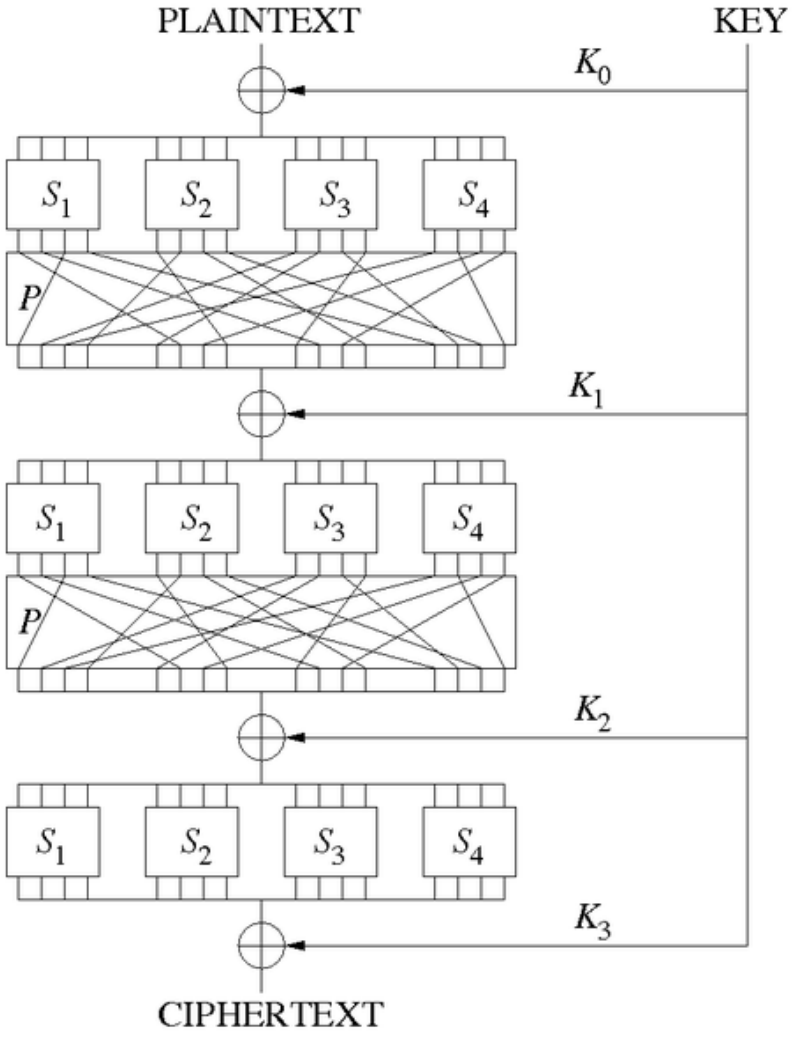


Exemplos:

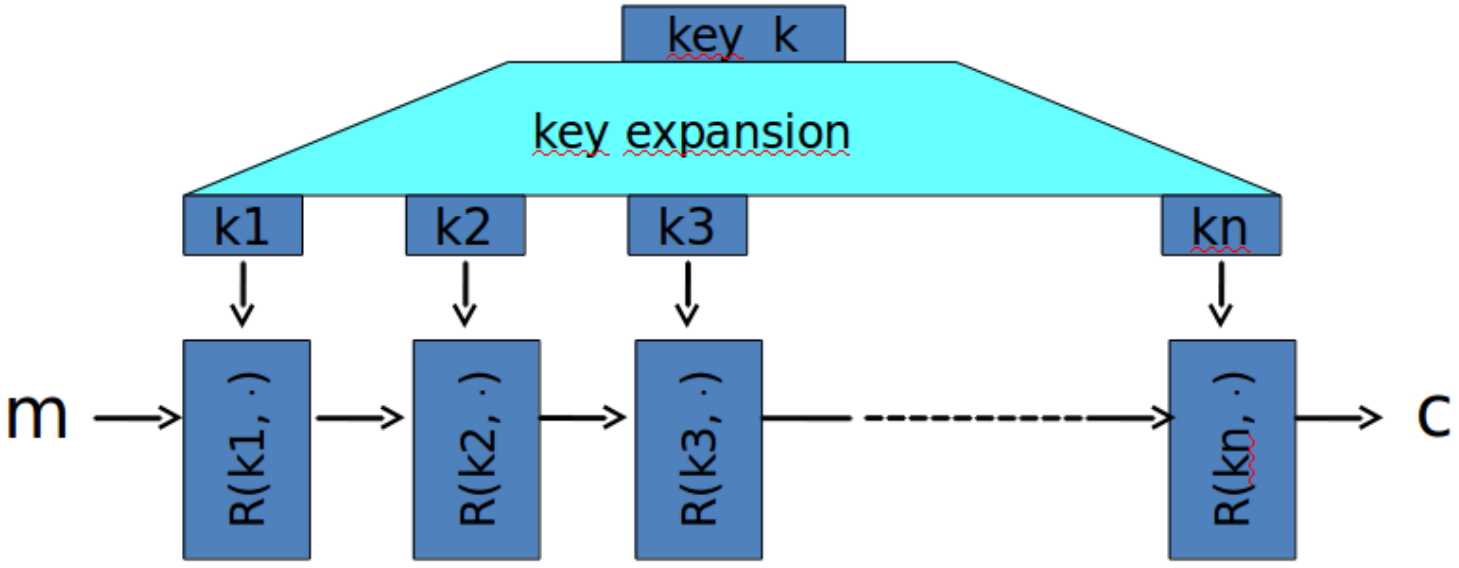
3DES $n = 64$ bits, $k = 168$ bits

AES $n = 128$ bits, $k = 128, 192$ e 256 bits

Criptografia de Blocos - 1 Bloco

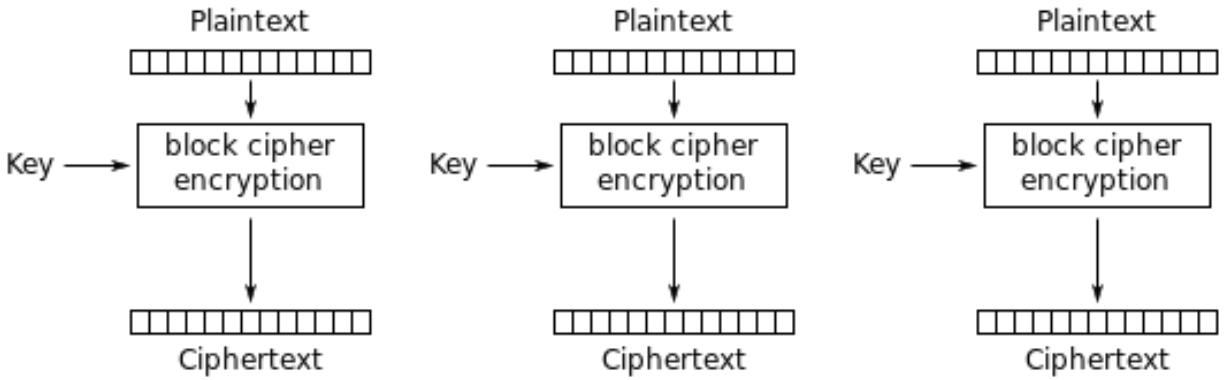


Criptografia de Blocos - 1 Bloco

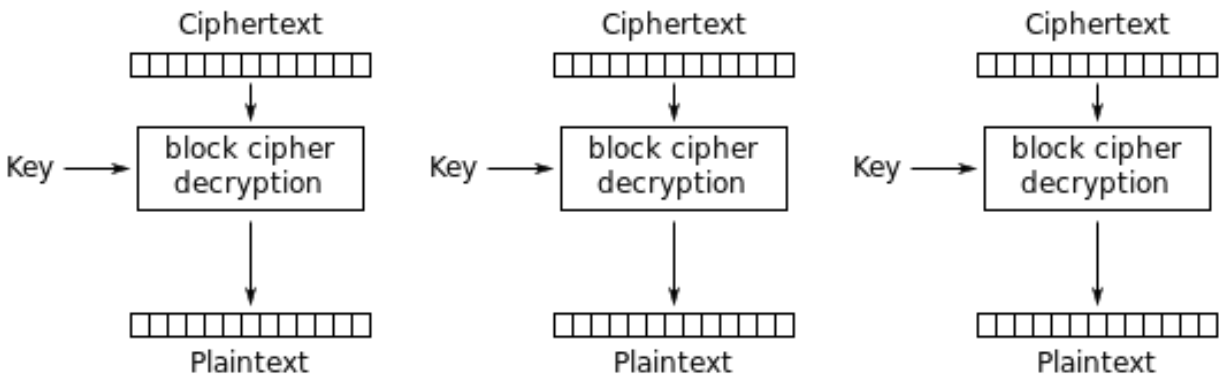


Criptografia de Blocos (Eletronic Code Book - ECB)

Criptografando uma mensagem maior que um bloco:



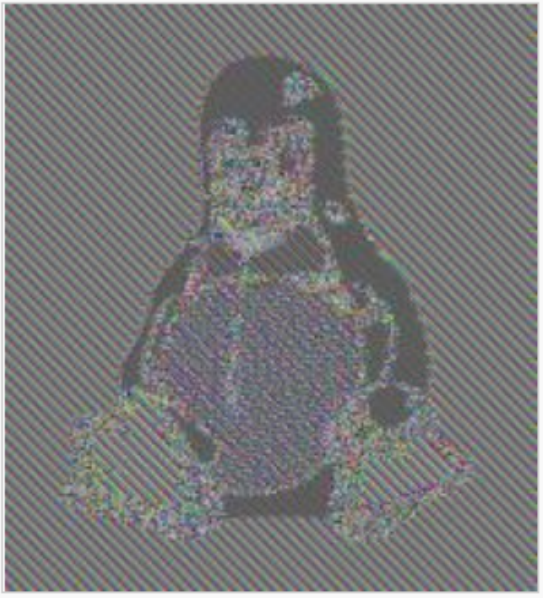
Electronic Codebook (ECB) mode encryption



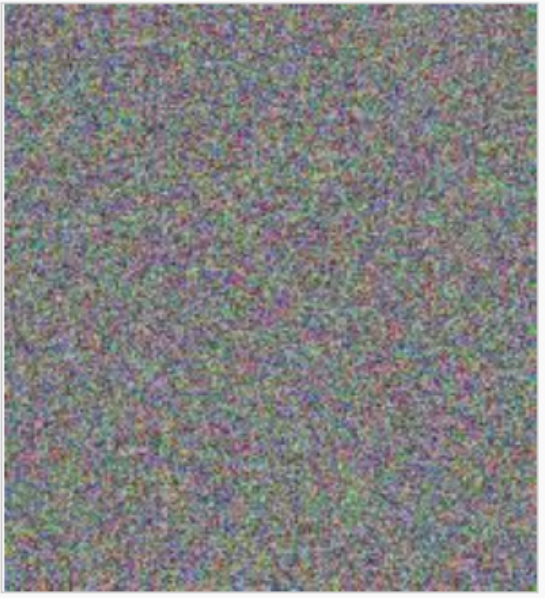
Universidade Estadual de Ponta Grossa

Criptografia de Blocos

Original image



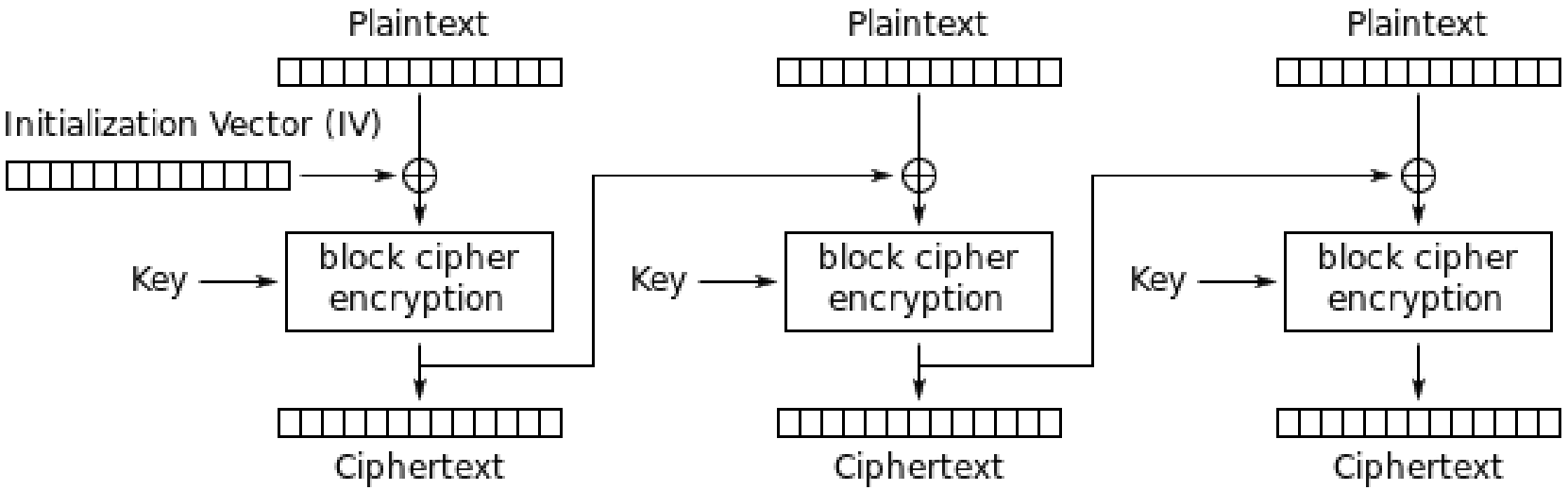
Encrypted using ECB mode



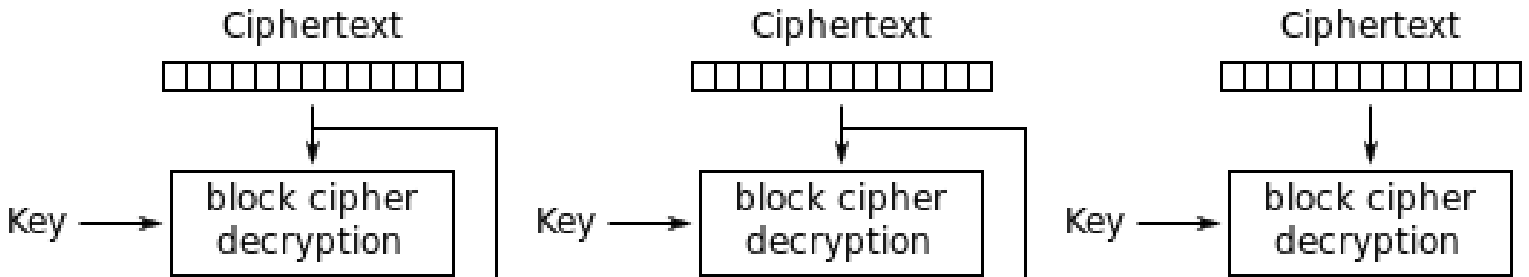
Modes other than ECB result in pseudo-randomness

Criptografia de Blocos (Cipher Block Chaining)

Criptografando uma mensagem maior que um bloco:

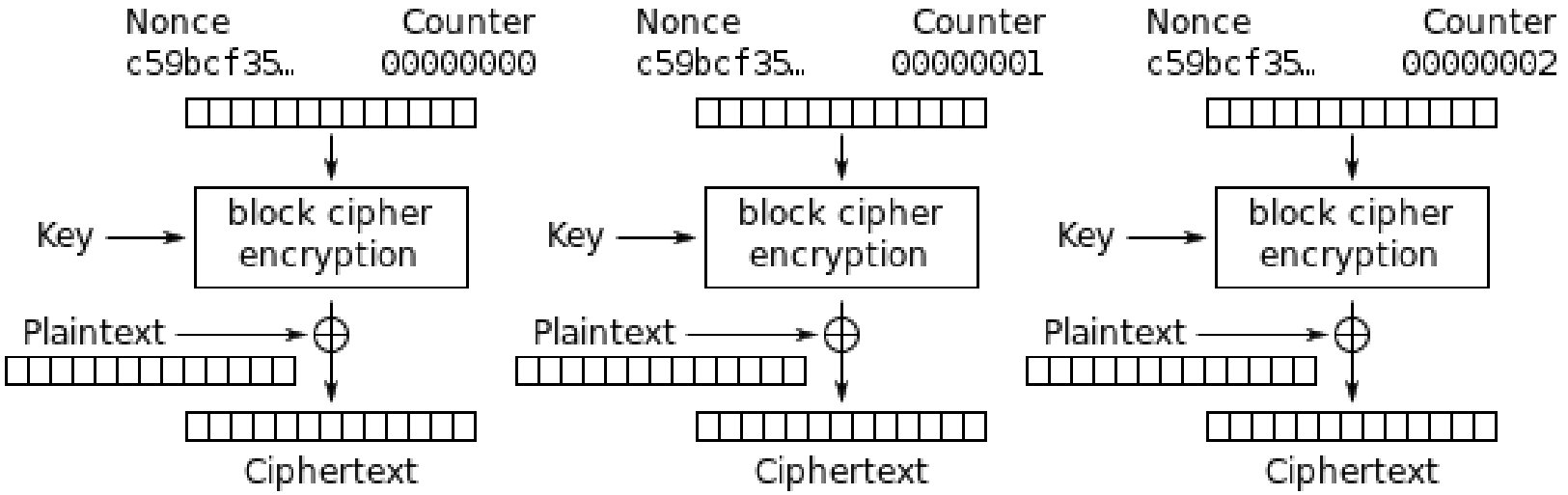


Cipher Block Chaining (CBC) mode encryption

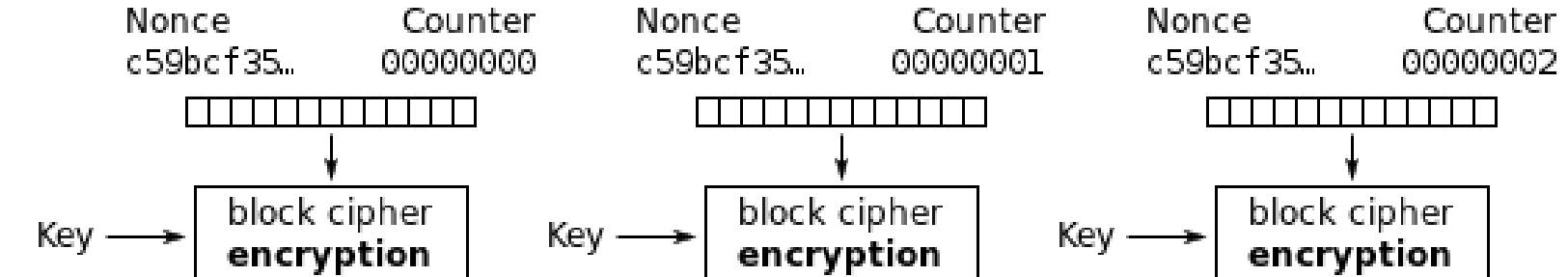


Criptografia de Blocos - CTR (Counter Mode)

Criptografando uma mensagem maior que um bloco:



Counter (CTR) mode encryption



Universidade Estadual de Ponta Grossa

Criptografia de Chave Pública, Integridade de Mensagens, Assinaturas Digitais

Os tópicos abaixo foram apresentados usando o quadro negro.
Cobrimos o capítulo 8 do livro de Kurose e Ross.

- Criptografia de Chave Pública
- Integridade de Mensagens
- Assinaturas Digitais
- Autoridades certificadores

- ver o livro do Kurose e Ross seções 8.1 até 8.3

SSL/TLS

- autenticação
- integridade
- privacidade

Universidade Estadual de Ponta Grossa

Histórico

- Computador eletrônico - Eniac 1946
- ARPANET - 1969
- TCP/IP - em uso em 1983