MSc - Cybersecurity

CMT310: Developing Secure Systems and Applications

Cryptography: Introduction, Symmetric Encryption AES, Modes of Operation

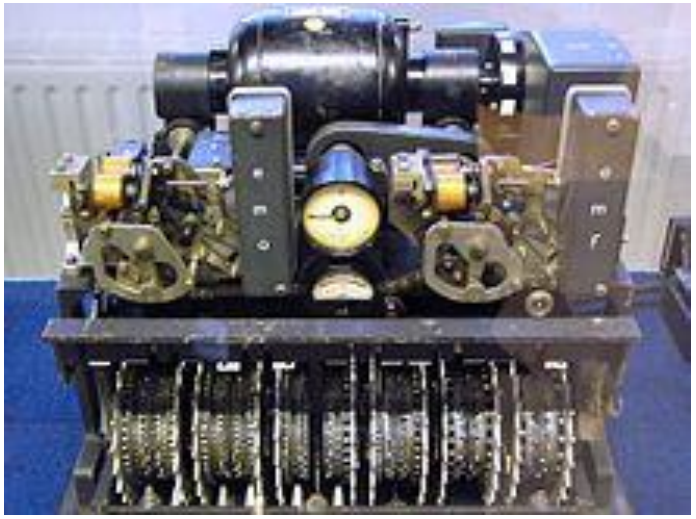
Dr Neetesh Saxena
saxenan4@cardiff.ac.uk

Cryptography

- Cryptography (secret writing) or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

History of Crytography

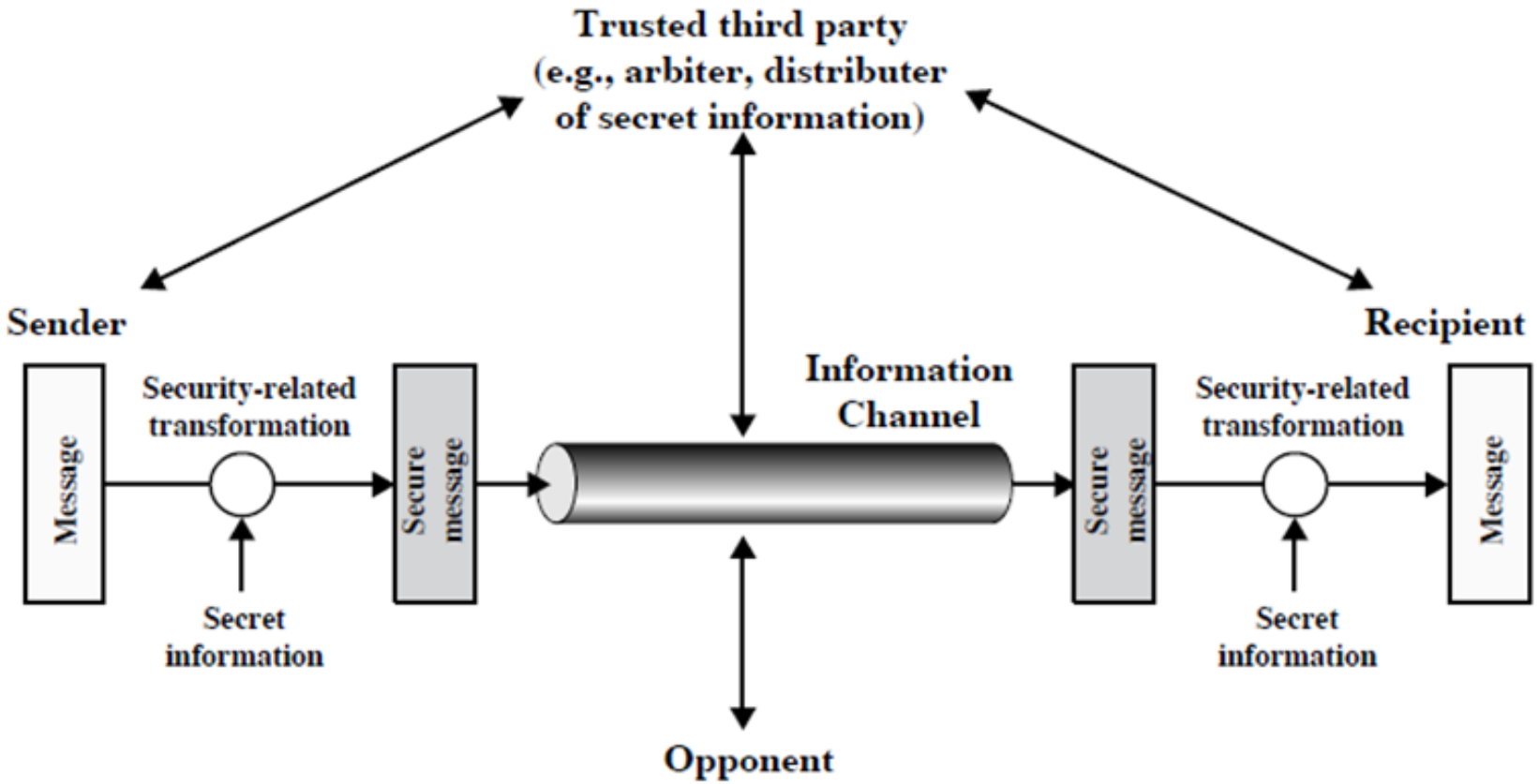
- Earliest recorded us around 1900BC in Egypt
- Around 100BC Julius Caesar used substitution cipher
- 1623 – Sir Francis Bacon described bilateral cipher
  - A type of steganography (hiding)
- Lots of other uses/advances – most notable Enigma machine in WWII
- 1970's - Dr. Horst Feistal invented DES
- 1977 magazine The Scientific American – RSA announced
- 2007 Quantum Cryptography successfully used to transmit 50 miles



German Lorenz cipher machine, used in World War II to encrypt messages.

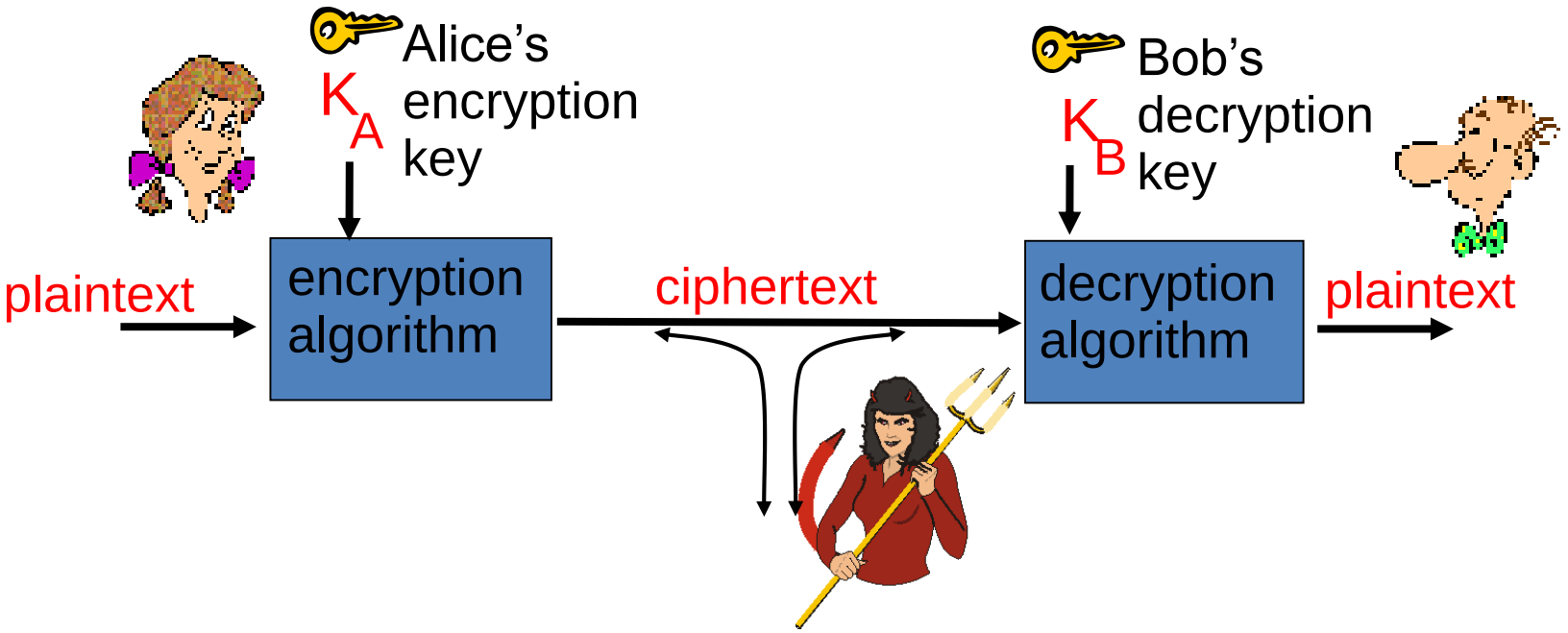
https://slideplayer.com/slide/9828075/

Model for Network Security



Model for Network Security

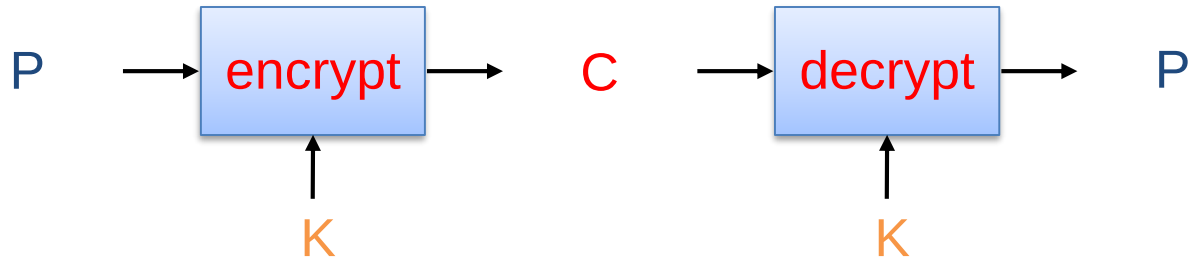
The Language of Cryptography



Symmetric key crypto: sender, receiver keys *identical*

Public-key crypto: encryption key *public*, decryption key *secret* (private)

Symmetric Cryptosystem

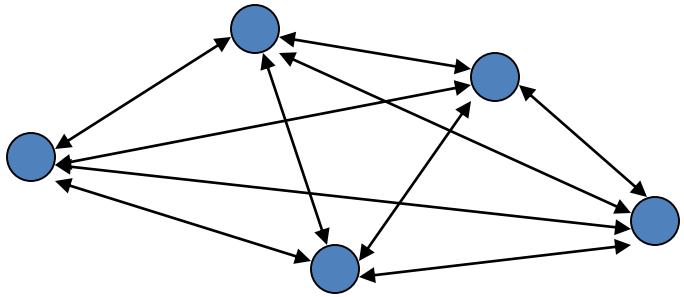


- Scenario
  - Alice wants to send a message (plaintext P) to Bob.
  - The communication channel is insecure
  - If Alice and Bob have previously agreed on a symmetric encryption scheme and a secret key K, the message can be sent encrypted (ciphertext C)
- Issues
  - What is a good symmetric encryption scheme?
  - What is the complexity of encrypting/decrypting?
  - What is the size of the ciphertext, relative to the plaintext?

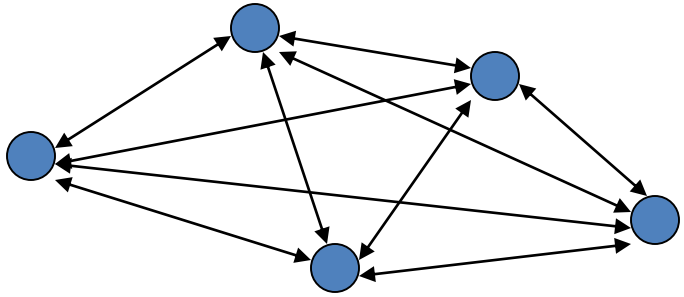
Limitations of Symmetric Cryptosystems

- Need of a secured channel to exchange the sensitive key information

- The “n-square” problem



The “n-square” Problem



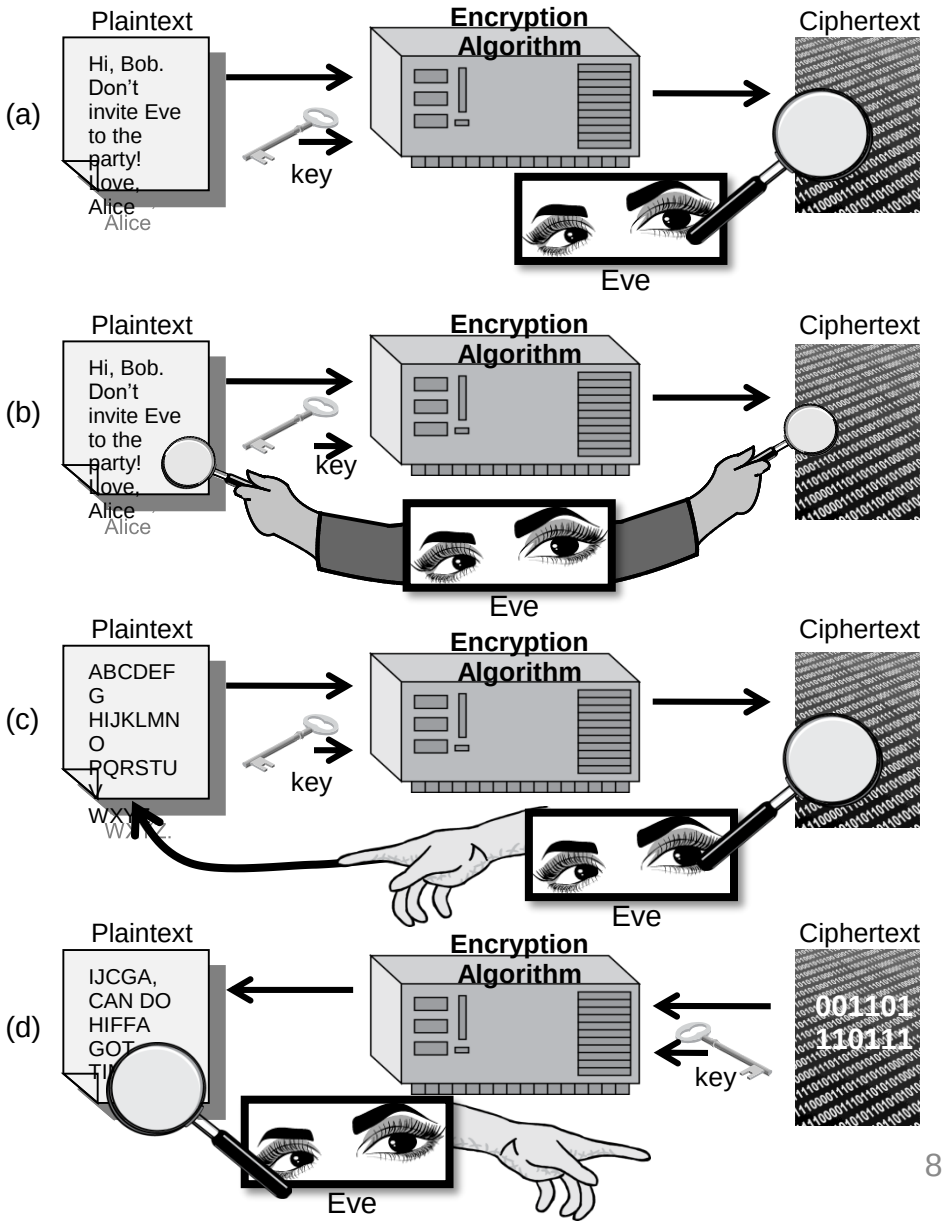
- for *n* users *n*(*n*-1)/2 keys must be exchanged:

$$\frac{n(n-1)}{2} = \frac{n^2 - n}{2}$$

- for *n*=8, number of keys=28
- for *n*=9, number of keys=36
- for *n*=1000, number of keys =499,500

Attacks – Attacker's Capabilities

- Attacker may have
  a) collection of ciphertexts (ciphertext only attack)
  b) collection of plaintext/ciphertext pairs (known plaintext attack)
  c) collection of plaintext/ciphertext pairs for plaintexts selected by the attacker (chosen plaintext attack)
  d) collection of plaintext/ciphertext pairs for ciphertexts selected by the attacker (chosen ciphertext attack)

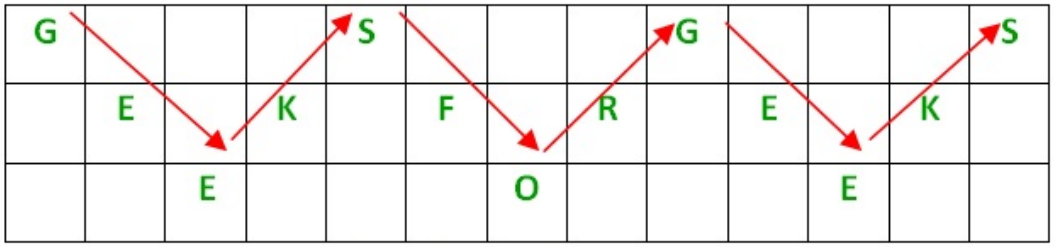


Brute-Force Attack

- Try all possible keys K and determine if $D_K(C)$ is a likely plaintext
  - Requires some knowledge of the structure of the plaintext
- Key - sufficiently long random value
  - to make exhaustive search attacks unfeasible

Classical Cryptography

- Transposition Cipher
  - Rail Fence cipher

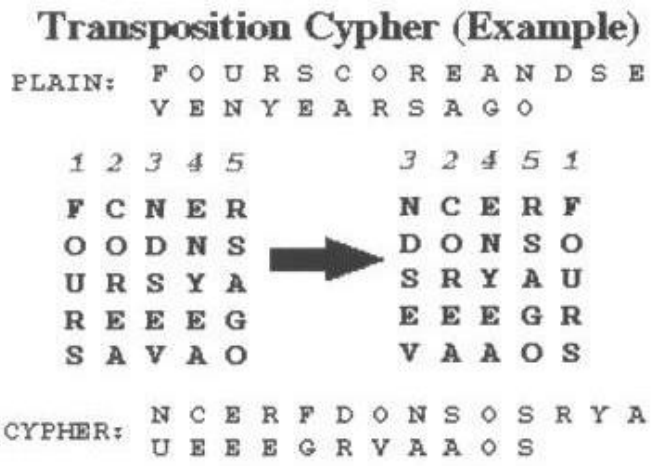


  - Columnar transposition

Given text = Geeks for Geeks
Keyword = HACK
Order of Alphabets in HACK = 3124

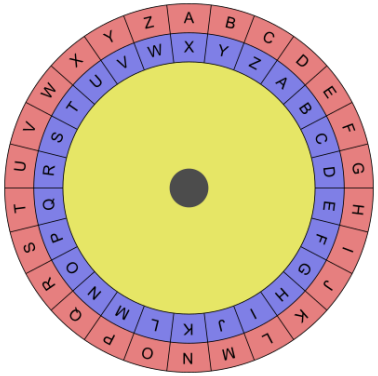
H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

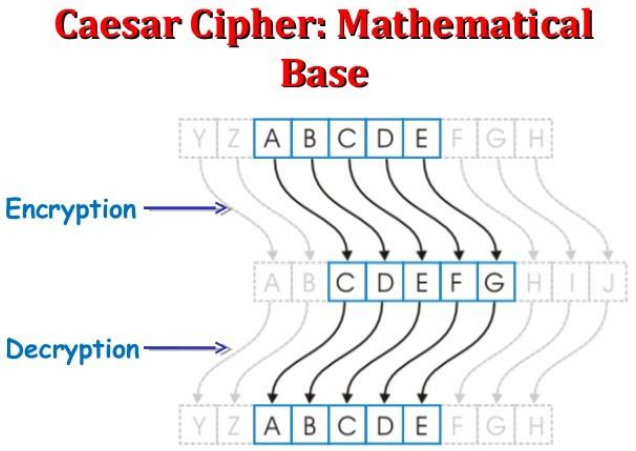
Print Characters of column 1,2,3,4
Encrypted Text = e kefGsGsrekoe_



Substitution Cipher

- Simple substitution cipher (Caesar cipher)
- Vigenere cipher (Polyalphabetic substitution)
- One-time pad





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

Plaintext: TECHNOLOGICAL UNIVERSITY

Key: HOUGHTON

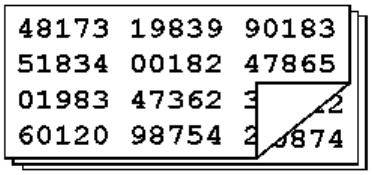
Key Length: HOUGHTONHOUGH TONHOUGNTO

Ciphertext: ASWNUHZBNWWG SNBVCSLYPM

Weaknesses of the One-Time Pad

- In spite of their perfect security, one-time pads have some weaknesses
- The key has to be as long as the plaintext
- Keys can never be reused
  - Repeated use of one-time pads allowed the U.S. to break some of the communications of Soviet spies during the Cold War.

Example One-Time Pad



Double agent claims sender used following "key"

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
"key":	101	111	000	101	111	100	000	101	110	000
"Plaintext":	011	010	100	100	001	010	111	100	000	101
	k	i	l	l	h	i	t	l	e	r

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Types of Symmetric Ciphers

- Block ciphers
  - operate on chunks of plaintext of specified length
- Stream ciphers
  - operate on one plaintext character at a time

Terminology

- Substitution and Permutation
  - substitution (S-box)
  - permutation (P-box)

- **Diffusion** – if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and vice versa

- **Confusion** – each bit of the ciphertext should depend on several parts of the key, obscuring the connections between the two.

Block Ciphers in Practice

- Data Encryption Standard (DES)
  - Developed by IBM and adopted by NIST in 1977
  - 64-bit blocks and 56-bit keys
  - Small key space makes exhaustive search attack feasible since late 90s
- Triple DES (3DES)
  - Nested application of DES with three different keys KA, KB, and KC
  - Effective key length is 168 bits, making exhaustive search attacks unfeasible
  - $C = E_{KC}(D_{KB}(E_{KA}(P)))$; $P = D_{KA}(E_{KB}(D_{KC}(C)))$
  - Equivalent to DES when KA=KB=KC (backward compatible)
- Advanced Encryption Standard (AES)
  - Selected by NIST in 2001 through open international competition
  - 128-bit blocks and several possible key lengths: 128, 192 and 256 bits
  - Exhaustive search attack not currently possible
  - AES-256 is the symmetric encryption algorithm of choice

RC2, RC5, and RC6 are symmetric-key block ciphers.

Block size

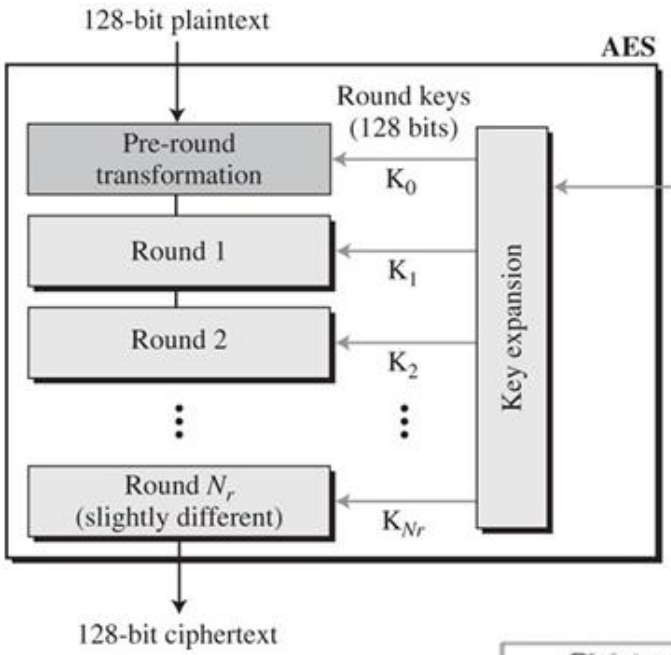
Normally the block size is fixed, and the block of ciphertext produced by the block cipher is usually also the same length as the plaintext block size.

Typical block sizes are 64 (DES) and 128 (AES).

1. What happens if the block size is “too short”?
2. What happens if the block size is “too long”?
3. Why are most block sizes multiples of 8?

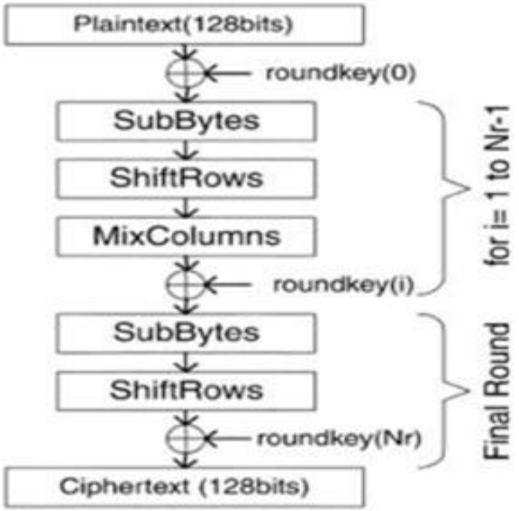
AES

AES Structure

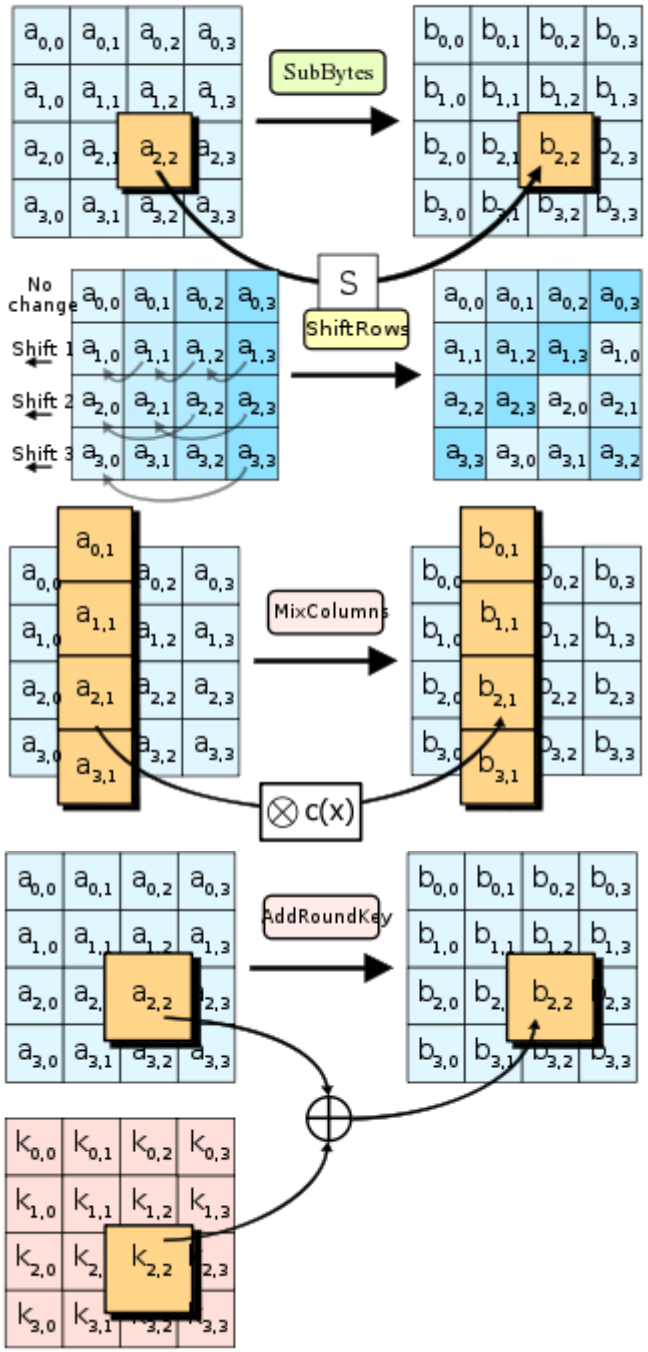


Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size



AES does bit manipulation

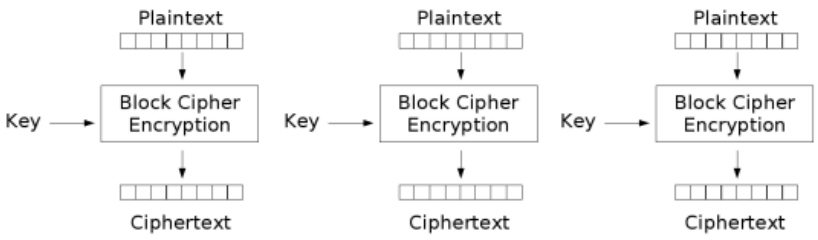


Modes of Operation

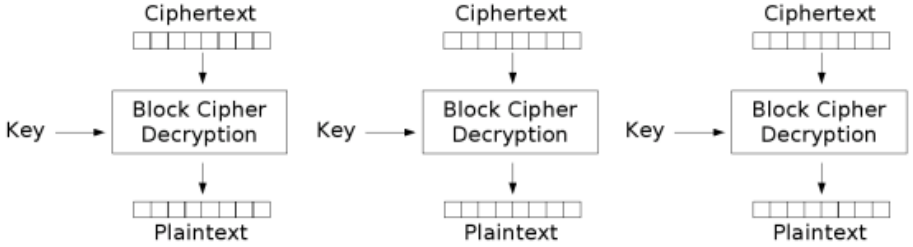
- Electronic Code Book, ECB
- Cipher Block Chaining, CBC
- Cipher Feedback Block CFB
- Output Feedback Block OFB
- Counter CTR

Block Cipher Modes

- A block cipher mode describes the way a block cipher encrypts and decrypts a sequence of message blocks.
- Electronic Code Book (ECB) Mode (is the simplest):
  - Block P[i] encrypted into ciphertext block $C[i] = E_K(P[i])$
  - Block C[i] decrypted into plaintext block $M[i] = D_K(C[i])$



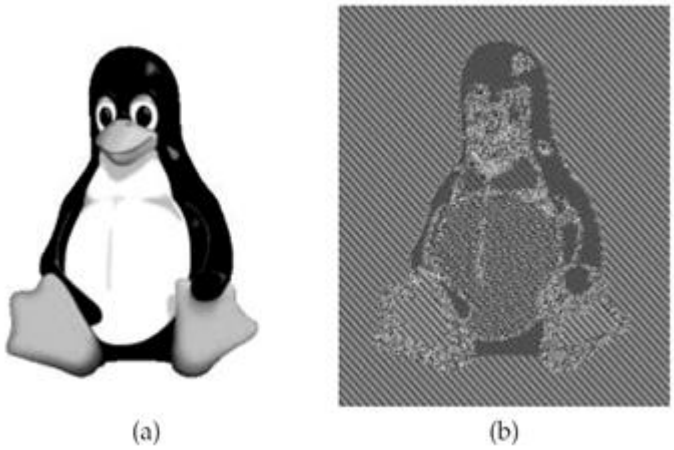
Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

Strengths and Weaknesses of ECB

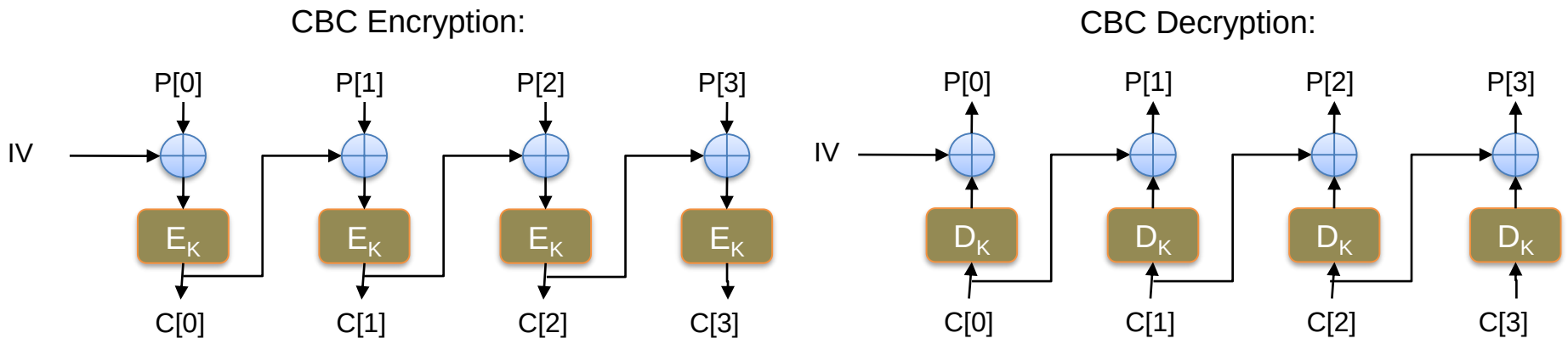
- Strengths:
  - Is very simple
  - Allows for parallel encryptions of the blocks of a plaintext
  - Can tolerate the loss or damage of a block
- Weakness:
  - Documents and images are not suitable for ECB encryption since patters in the plaintext are repeated in the ciphertext.



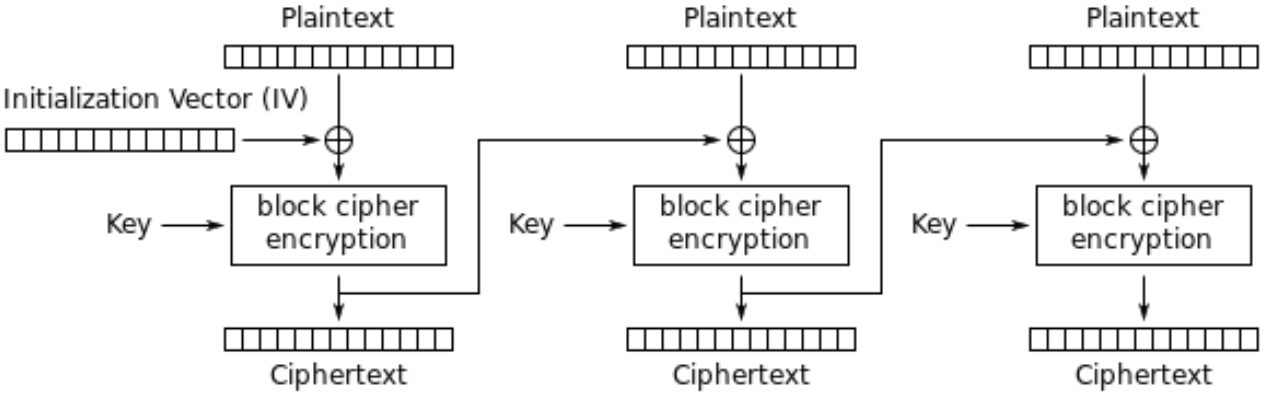
(a) (b)

Cipher Block Chaining (CBC) Mode

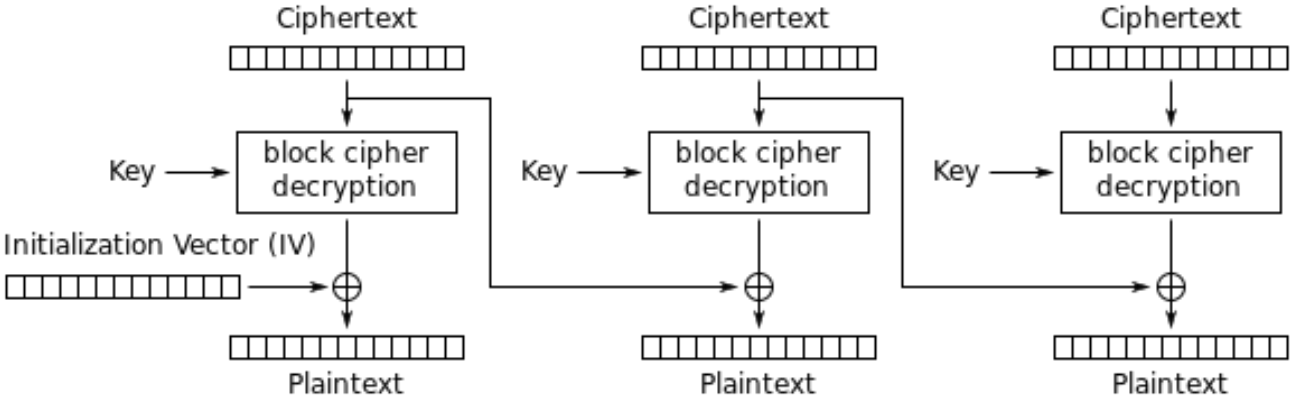
- In Cipher Block Chaining (CBC) Mode
  - The previous ciphertext block is combined with the current plaintext block $C[i] = E_K(C[i-1] \oplus P[i])$
  - $C[-1] = V$, a random block separately transmitted encrypted (known as the initialization vector)
  - Decryption: $P[i] = C[i-1] \oplus D_K(C[i])$



CBC



Cipher Block Chaining (CBC) mode encryption

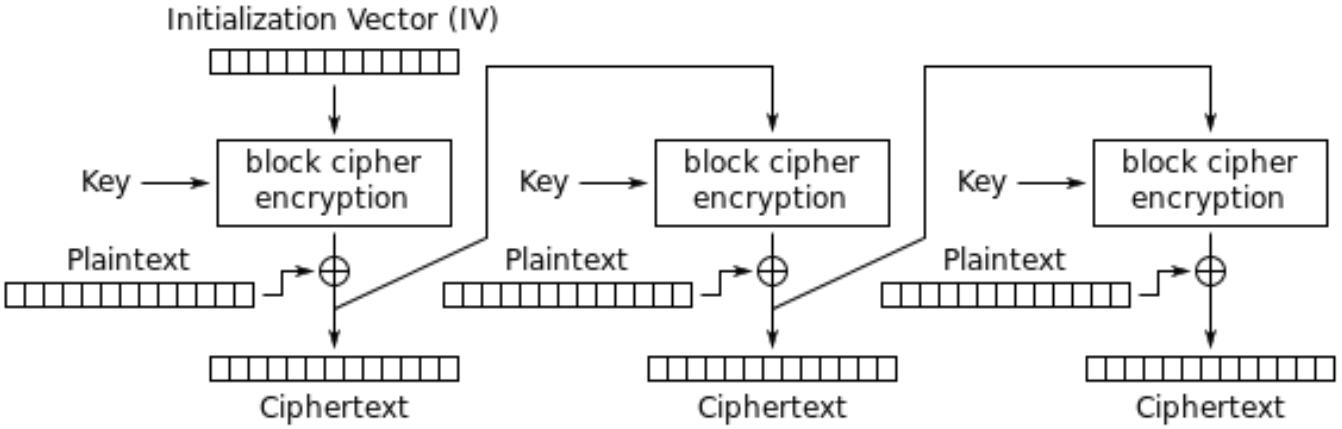


Cipher Block Chaining (CBC) mode decryption

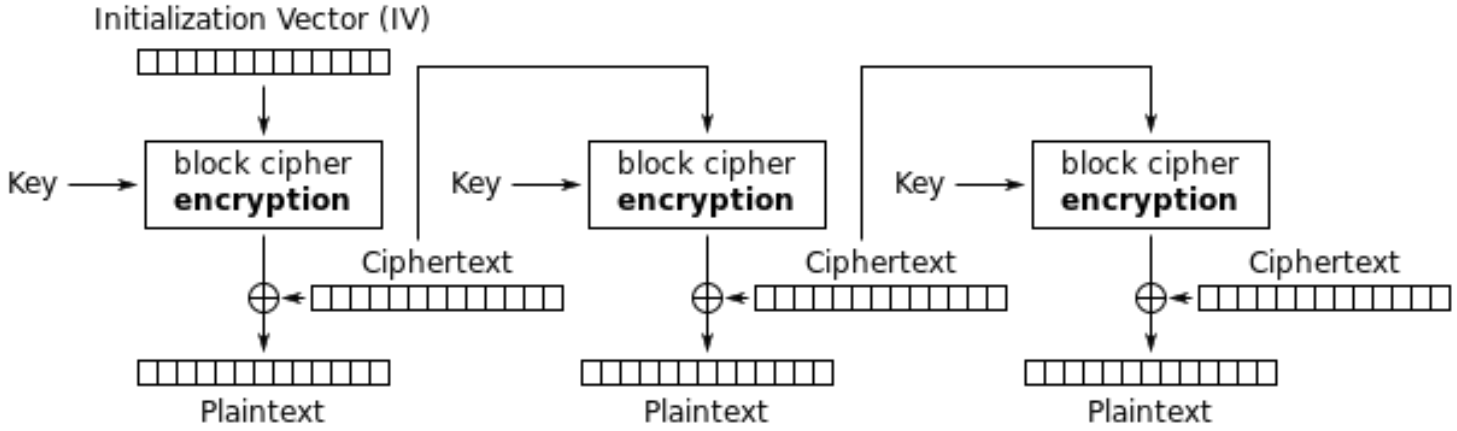
Strengths and Weaknesses of CBC

- Strengths:
  - Doesn’t show patterns in the plaintext
  - Is the most common mode
  - Is fast and relatively simple
- Weaknesses:
  - CBC requires the reliable transmission of all the blocks sequentially
  - CBC is not suitable for applications that allow packet losses (e.g., music and video streaming)

CFB Mode

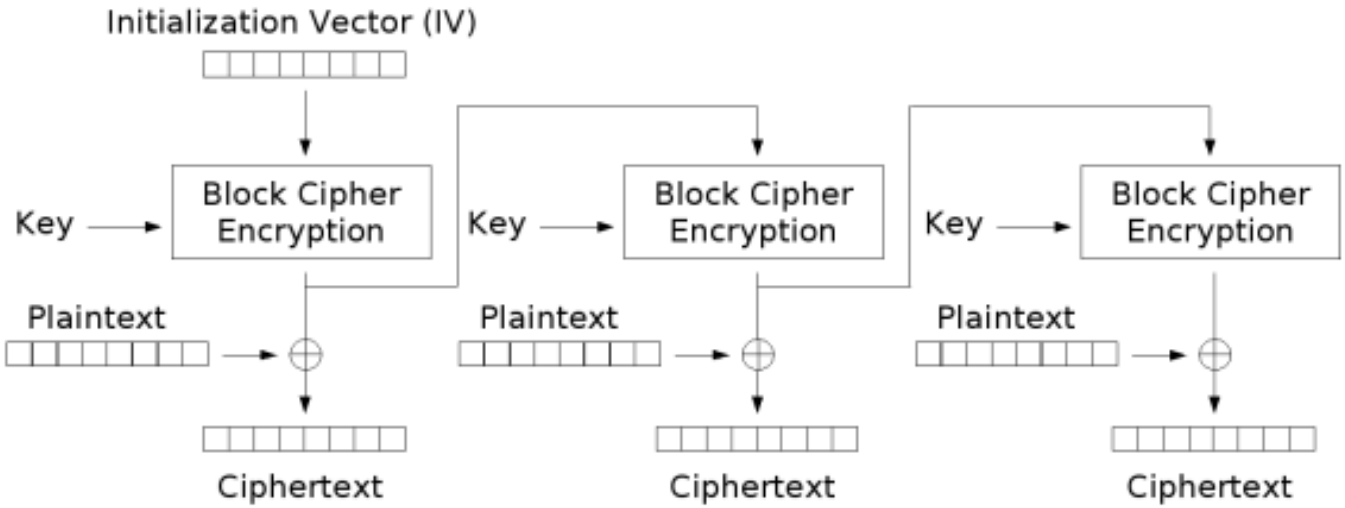


Cipher Feedback (CFB) mode encryption

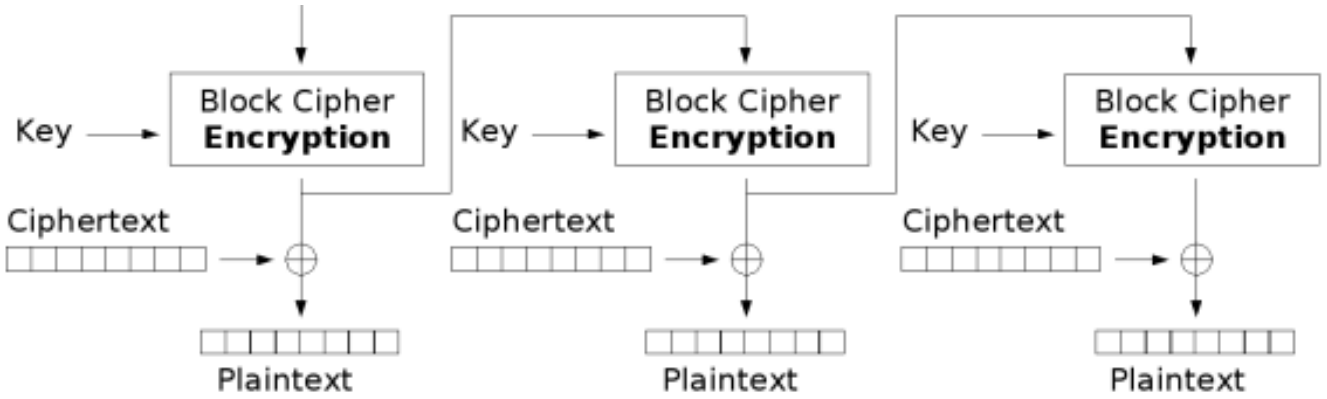


Cipher Feedback (CFB) mode decryption

OFB Mode



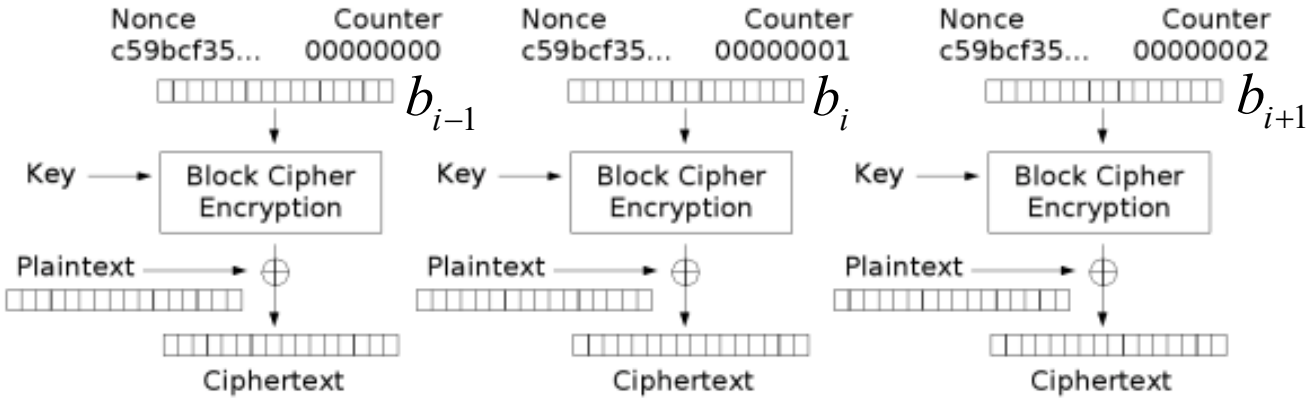
Output Feedback (OFB) mode encryption



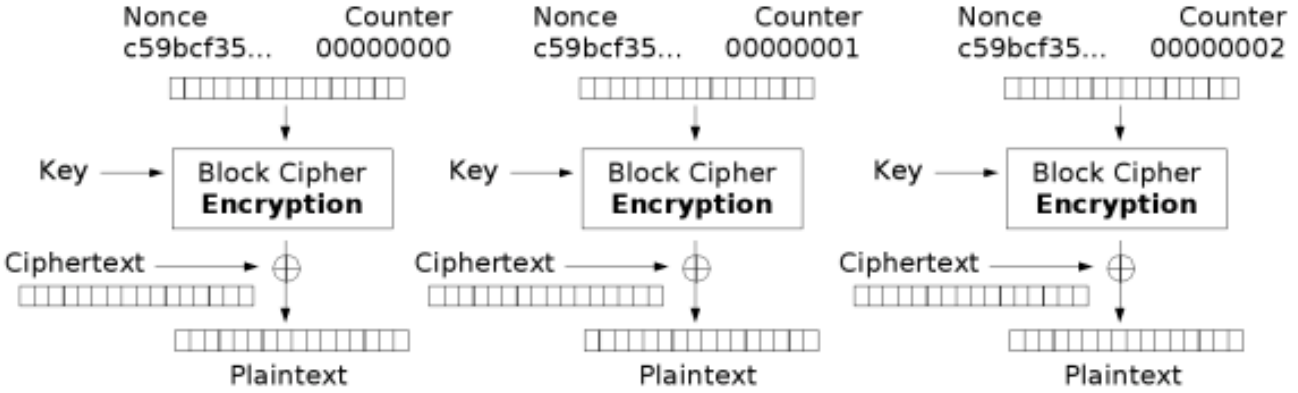
Output Feedback (OFB) mode decryption

Counter Mode

- Register as nonce and counter
- Supports “random access”



Counter (CTR) mode encryption



Counter (CTR) mode decryption

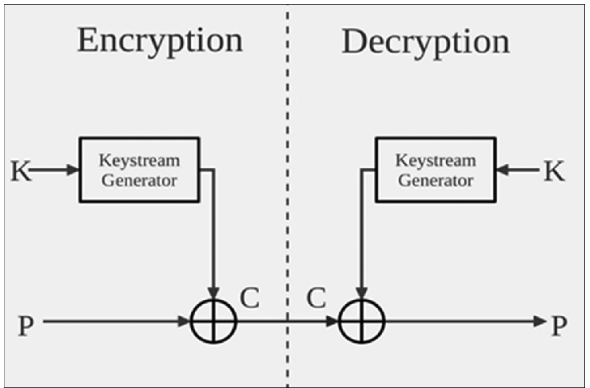
Characteristics of OFB/CFB/Counter

- Losing Synchronicity in OFB is fatal
  - All later decryptions will be garbled (blocks will be inserted or removed)
- *Advantage* - OFB *does* have over CFB - can pre-generate the keystream (and pass to the next block), since it does not depend on the plaintext.
- CBC vs. CFB – encryption mode for decryption
- Counter mode lets you generate a bit in the middle of the stream
- CTR, CFB and OFB convert block cipher into stream cipher.

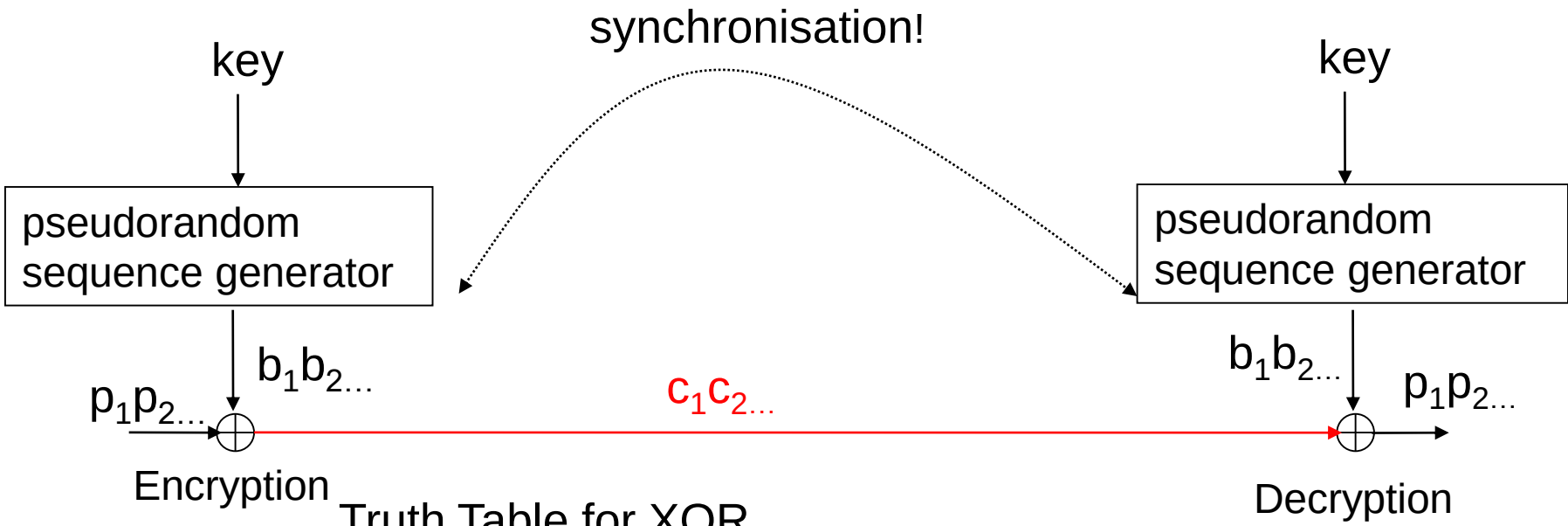
Stream Cipher

- Key stream
  - Pseudo-random sequence of bits S = S[0], S[1], S[2], …
  - Can be generated online one bit (or byte) at the time
- Stream cipher
  - XOR the plaintext with the key stream C[i] = S[i] ⊕ P[i]
  - Suitable for plaintext of arbitrary length generated on the fly, e.g., media stream
- Synchronous stream cipher
  - Sender and receiver must synchronize in using key stream
  - Only a single digit in the plaintext is affected in case of error
  - Does not propagate to other parts of the message.

- e.g., RC4: Symmetric key stream cipher.



Stream Ciphers



Truth Table for XOR

p	b	p⊕b
0	0	0
0	1	1
1	0	1
1	1	0

self-cancelling property:
y⊕y=0
sender: c=p ⊕b
receiver: c ⊕b= (p ⊕b) ⊕b=p

Stream Ciphers

- Strengths
  - high speed
- Weaknesses
  - low security
  - synchronisation issues
- Applications
  - video data encryption
  - mobile communications
  - encrypt satellite communications

Security Goals and Properties

- Mutual Authentication
  - The server must authenticate the user and the user should be able to verify that it is connected to the legitimate server.
  - Defeats the redirection and impersonation attacks.

- Perfect Forward Secrecy (PFS)
  - A scheme maintains PFS if no adversary A in time t can retrieve the past session keys k, even the long term keys LTK (i.e., the private key of the user or a session key) are compromised.

Security Goals and Properties

- Information Confidentiality
  - Encrypted message sent by the user must be indistinguishable from a randomly generated messages, and supports Indistinguishability under Chosen Plaintext Attack (IND-CPA).

- Message Integrity
  - Integrity of each message can be achieved using a well known Collision-Resistant Hash Functions (CRHF).

$H : \{0,1\}^n \to \{0,1\}^m$ $(m<n)$ is a collision-resistant hash function if it there exists a negligible function ϵ such that for all security parameters $n \in \mathbb{N}$,

$$Pr[(msg_0, msg_1) \leftarrow \mathcal{A}(1^n, h) : msg_0 \neq msg_1 \wedge h(msg_0) = h(msg_1)] \leq \epsilon(n).$$

Cont.

- Untraceability
  - Untraceability is maintained if A cannot distinguish whether two generated messages correspond to the same or two different identities of the users.
    - Forward untraceability
    - Backward untraceability

- Forward privacy
  - Similar to untraceability with additional capability.
  - One of two messages is given to adversary A. Clearly, now A can trace the user's identity and/or other information.
  - Forward privacy is maintained if A is still unable to trace previous sessions (without giving a secret or session key).

- Anonymity is maintained if only the sender and the intended receiver can know the actual identity of the user.

Summary

- Basics – cryptography
- Types of attacks – capabilities
- Modes of operations
- Symmetric key cryptography
- Security Goals and Properties