NCC education Awarding Great British Qualifications

Network Security and Cryptography

Topic 2: Lecture 1

Classical Symmetric Cryptography

The Unit Roadmap

Unit Aim: The unit aims to provide a comprehensive understanding of the fundamental principles, techniques, and best practices employed to safeguard computer networks from cyber threats. It explores the concepts of secure communication, cryptographic algorithms, encryption, and authentication protocols, etc. equipping learners with essential knowledge to protect network infrastructure and data integrity in an increasingly interconnected digital landscape.

Unit Syllabus

- Introduction to Network Security and Cryptography
- **Cryptography Techniques**
- Operating System Security and Vulnerabilities
- Software Vulnerabilities and attacks
- Network Security and Defense
- Email and Web Security
- Firewalls
- VLAN and VPN
- Wireless Security
- Information Security Management

Scope and Coverage

This topic will cover:

- Classical Symmetric Cryptography
- Modern Symmetric Cryptography

Learning Outcomes

By the end of this topic students will be able to:

- Demonstrate a systematic understanding of the concept of cryptography.
- Understand different classic cryptographic techniques.
- Understand the modern symmetric key encryption principles.
- Understand in detail different symmetric cryptography algorithms.

Last Topic

- In today's digital world, protection against cyber threats is curial.
- Protecting against cyber attacks involves implementing information security, cybersecurity, network security.
- Key characteristics of information that must be protected: Confidentiality, Integrity, Availability, Authenticity, Accountability and Non-repudiation.
- Common types of attacks: Interruption, Interception, Modification, Fabrication.
- At each layer of OSI model, there is a potential threat that need to be addressed.
- Cryptography is a techniques to address the security threats.
- Cryptography: Science of transforming information into secure form such that unauthorized persons cannot access it.

Quiz

1. What is Network Security?

a) Software that speeds up internet connections

b) Measures to protect computer networks

c) A type of computer virus

d) Social media privacy settings

Quiz

2. What does the "C" in CIA stand for in the context of information security?

a) Control

b) Confidentiality

c) Cryptography

d) Connectivity

Quiz

3. Which of the following is a key aspect of ensuring data integrity?

a) Availability

b) Encryption

c) Data backup

d) Non-repudiation

Quiz

4. Which of the following is a measure to maintain data confidentiality?

a) Hashing

b) Access control

c) Redundancy

d) Data mirroring

Quiz

5. Non-repudiation is associated with which aspect of the CIA triad?

a) Confidentiality

b) Integrity

c) Availability

d) Authentication

Symmetric Cryptography

A **single secret key** between the two communicating entities.

- Encrypt/decrypt a message using the same key
- Key: a piece of information or sequence of bits

Symmetric key rely on using some **secure method** whereby User A and User B can first agree on a secret key that is known only to them.

Classical Symmetric Ciphers

- Classical ciphers are historical cryptographic techniques used to encrypt and decrypt messages in the pre-computer era.

- Classical ciphers primarily rely on simple **substitution** and **transposition** techniques to achieve confidentiality.

Substitution Ciphers

- Letters of plaintext are replaced by other letters or by numbers or symbols

- Plaintext is viewed as a sequence of bits, then substitution replaces plaintext bit patterns with ciphertext bit patterns

Caesar Cipher

- Earliest known substitution cipher
- Replaces each letter by 3rd letter on

Example:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

Caesar Cipher

Define transformation as:

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

Mathematically give each letter a number

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then have Caesar cipher as:

$$C = E(p) = (p + k) \bmod (26)$$

$$p = D(C) = (C - k) \bmod (26)$$

Cryptanalysis of Caesar Cipher

- Only have 25 possible ciphers
  A maps to B,..Z

- Given ciphertext, just try all shifts of letters

- Do need to recognize when have plaintext

- E.g., **break ciphertext "GCUA VQ DTGCM"**

Try with shift 2
Answer: Easy to Break

Monoalphabetic Cipher

- Rather than just shifting the alphabet
- Could shuffle (jumble) the letters arbitrarily
- Each plaintext letter maps to a different random ciphertext letter
- Key is 26 letters long

```
Plain:   abcdefghijklmnopqrstuvwxyz
Cipher:  DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext:  ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
```

Monoalphabetic Cipher Security

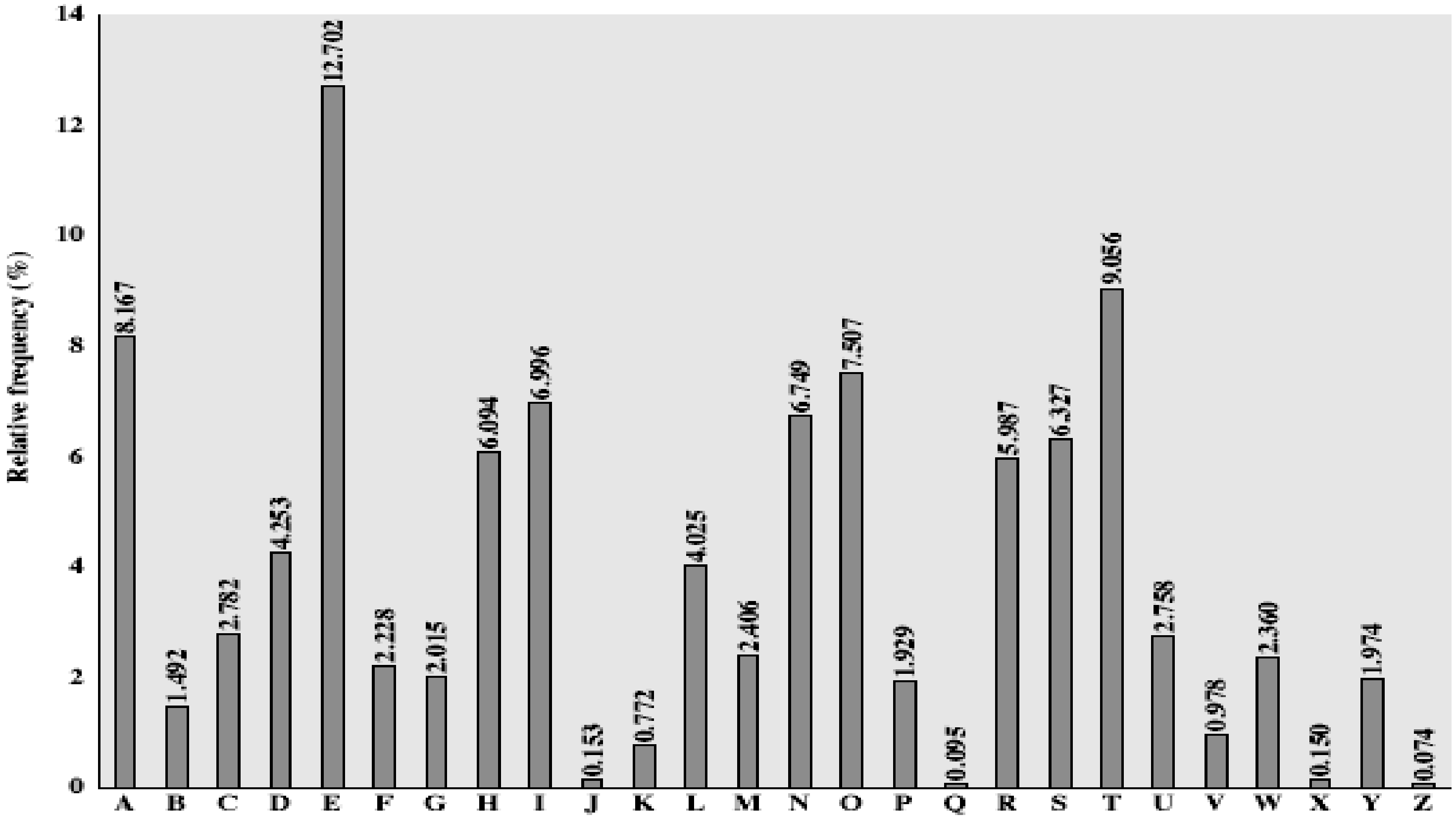
Now have a total of 26! = 4 x 10^{26} keys

Is that secure?

Problem is language characteristics

- Human languages are redundant
- Letters are not equally commonly used

English Letter Frequencies



Note that all human languages have varying letter frequencies, though the number of letters and their frequencies varies.

Example Cryptanalysis

Given ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

Count relative letter frequencies (see text)

Guess P & Z are e and t

Guess ZW is th and hence ZWP is the

Proceeding with trial and error finally get:

```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

One-Time Pad

- If a truly random key as long as the message is used, the cipher will be secure - One-Time pad
- E.g., a random sequence of 0’s and 1’s XORed to plaintext, no repetition of keys
- Unbreakable since ciphertext bears no statistical relationship to the plaintext
- For any plaintext, it needs a random key of the same length
  - ✓Hard to generate large amount of keys
- Have problem of safe distribution of key

Transposition Ciphers

- Now consider classical transposition or permutation ciphers
- These hide the message by rearranging the letter order, without altering the actual letters used
- Can recognize these since have the same frequency distribution as the original text

Rail Fence Cipher

Write message letters out diagonally over a number of rows

Then read off cipher row by row

E.g., write message out as 2 rail: “Meet me after the class”

```
m e m a t r h c a s
 e t e f e t e l s
```

Giving ciphertext

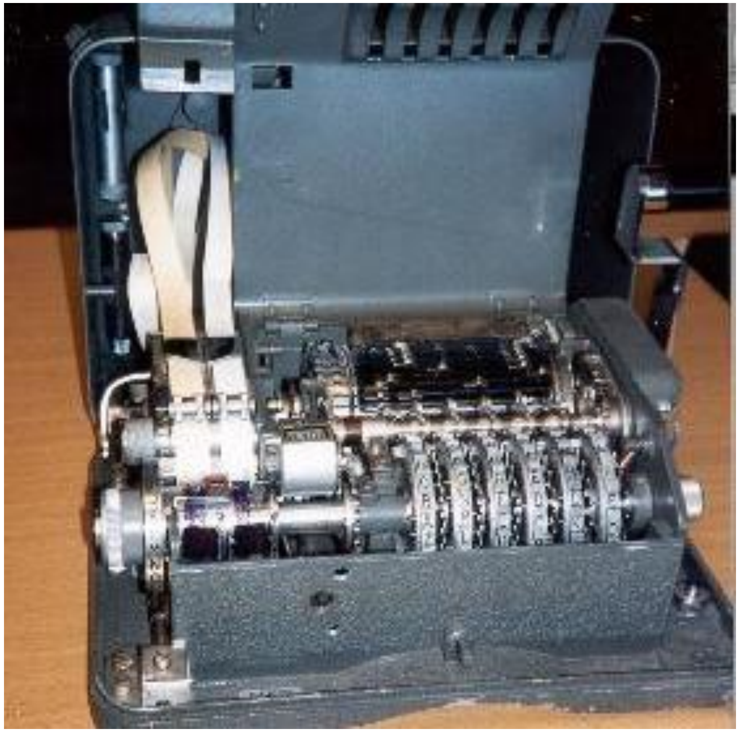
```
mematrhcasetefetels
```

Product Ciphers

- Ciphers using substitutions or transpositions are not secure because of language characteristics
- Hence consider using several ciphers in succession to make harder, but:
  - ✓ Two substitutions make another substitution
  - ✓ Two transpositions make a more complex transposition
  - ✓ But a substitution followed by a transposition makes a new much harder cipher
- This is bridge from classical to modern ciphers

Rotor Machines

- Before modern ciphers, rotor machines were most common complex ciphers in use
- Widely used in WW2 - German Enigma, Allied Hagelin, Japanese Purple
- Implemented a very complex, varying substitution cipher



Cryptanalysis

- The main objective of an attacker is to recover the key rather than the plaintext.
- Relies on knowledge of the nature of the algorithm plus knowledge of the plaintext or access to some plaintext/ciphertext pairs.
- An encryption scheme is computationally secure if:
- The cost of breaking the scheme exceeds the value of the encrypted information.
- The time required to break to the scheme is more than lifetime of the information.

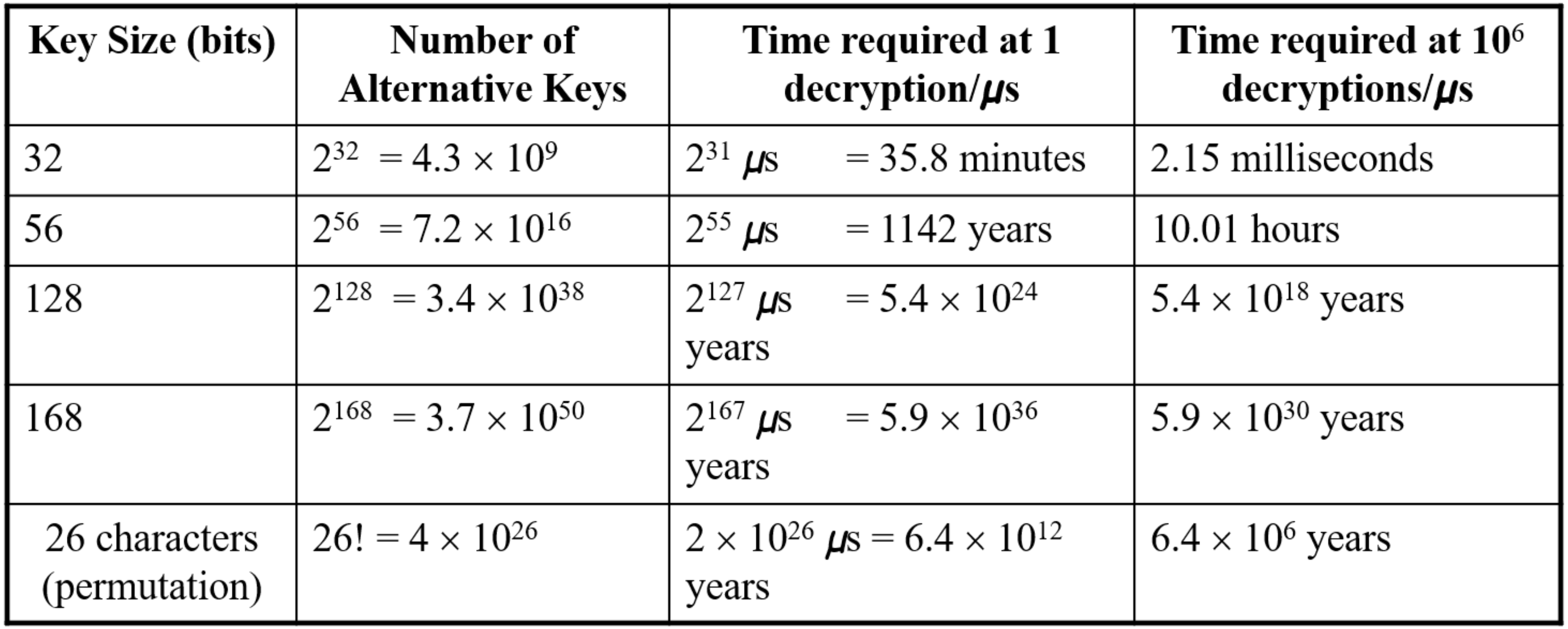
Cryptanalysis Schemes

- Ciphertext only:
  - ✓ Exhaustive search until “recognizable plaintext”
  - ✓ Need enough ciphertext
- Known plaintext:
  - ✓ Secret may be revealed (by spy, time), thus <ciphertext, plaintext> pair is obtained
  - ✓ Great for monoalphabetic ciphers
- Chosen plaintext:
  - ✓ Choose text, get encrypted
  - ✓ Pick patterns to reveal the structure of the key

Brute Force Attacks

- Try every possible key until correct translation of the encrypted text into plaintext is obtained.
- The problem is the time required to do this.
- On average, an attacker must try half of all possible keys before successfully translating a ciphertext.

Brute Force Attacks



Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

STALLINGS, W. 2022. *Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition*, Pearson.

Class Activity 1

Decrypt the following Rail Fence cipher with three rails:

Ciphertext: "**WECRUO ERDSOEERNTNE AIVDAC**"

Checkpoint Summary

- Classical ciphers primarily rely on simple substitution and transposition techniques to achieve confidentiality.
- Substitution cipher: Letters of plaintext are replaced by other letters or by numbers or symbols.
- Transposition cipher: Hide the message by rearranging the letter order, without altering the actual letters used.
- Can easily decrypt due to letter frequency.

Network Security and Cryptography

Topic 2: Lecture 2

Symmetric Key Cryptography

Modern Symmetric Cryptography

Modern symmetric encryption algorithms can be classified into two main categories:

- **Block ciphers** use algorithms to encrypt and decrypt a fixed-size block of plaintext and ciphertext, respectively, usually a multiple of 64 bits.
- **Stream ciphers** continuously encrypt any amount of data as it is presented, usually by mathematically combining the data with a keystream, an infinitely long key sequence that is generated based on a finite key starting value.

Block Cipher Principle

- Most symmetric block ciphers are based on a **Feistel Cipher Structure**
- Block ciphers look like an extremely large substitution
- Would need table of 264 entries for a 64-bit block
- Instead create from smaller building blocks
- Using idea of a product cipher

The fundamental principle of block ciphers is to take a fixed-size block of plaintext and transform it into a fixed-size block of ciphertext using a secret key.

Feistel Cipher Structure

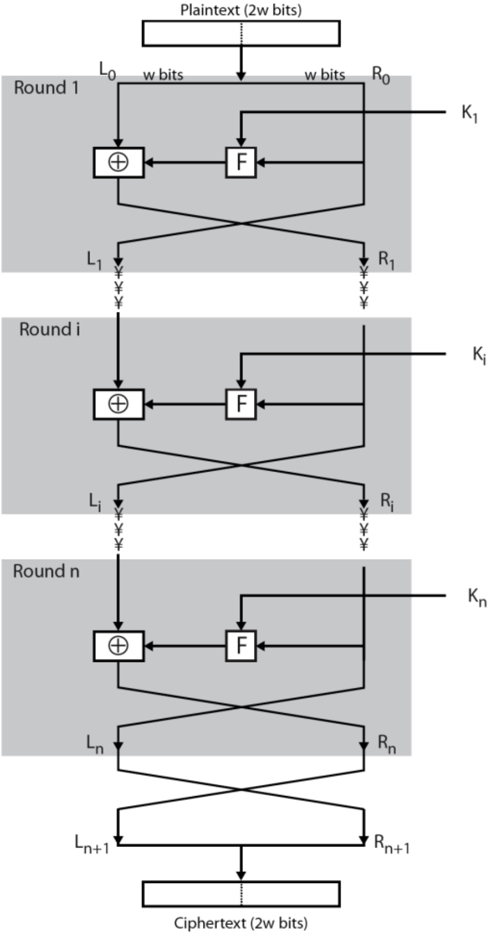
Feistel Cipher implements Shannon's S-P network concept based on invertible product cipher.

Key Characteristics of the Feistel Cipher Structure:

Block Division: The plaintext is divided into two equal-sized blocks, typically denoted as "L" (left half) and "R" (right half).

Multiple Rounds: The encryption process involves multiple rounds (typically 16 or 32 rounds), with each round applying different cryptographic functions to the left and right halves of the block.

Round Function: In each round, a round function is applied to the right half of the block, taking as input the right half and a round key derived from the main secret key. The output of the round function is then XORed with the left half.

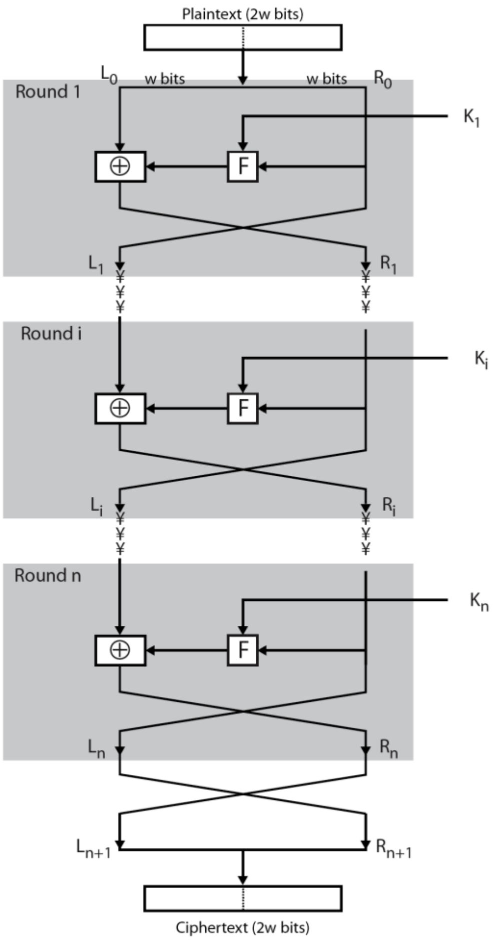


STALLINGS, W. 2022. *Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition*, Pearson.

Feistel Cipher Structure

Swap: After the XOR operation, the left and right halves are swapped for the next round. In other words, the left half of the current round becomes the right half for the next round, and vice versa.

Final Round: The final round is special, and it may differ from the regular rounds. Sometimes, the swap step is skipped in the last round, or an additional permutation is applied to the output to produce the final ciphertext.



Example of Block Ciphers

- Data Encryption Standard (DES),
- Advanced Encryption Standard (AES)

Data Encryption Standard (DES)

- A standardized encryption algorithm approved by the U.S. government in 1977.
- It uses a 56-bit key, which is sometimes stored with additional parity bits, extending its length to 64 bits.
- DES is a block cipher and encrypts and decrypts 64-bit data blocks.
- It is now considered insecure.
- In 1998, a cracker could crack the key in 3 days.

Advanced Encryption Standard (AES)

- AES replaced DES.
- A fast block cipher, with variable key length and block sizes (each can be independently set to 128, 192 or 256 bits).
- An official U.S. government standard since 2002.
- Now widely used for commercial and private encryption purposes.
- The algorithm is public, and its use is unrestricted.
- AES is used in TLS/SSL.

Advanced Encryption Standard (AES)

- Design uses theory of finite fields, a branch of algebra.
- Every block of 128 bits is presented as 4 by 4 array of bytes.
- Every round except start and end has 4 steps:
  - ✓ Substitution
  - ✓ Shift Rows
  - ✓ Mix Columns
  - ✓ Add Round Key

AES – Stage 1

- **KeyExpansion** - round keys are derived from the cipher key
- **Initial Round**

  AddRoundKey - each byte of the state is combined with the round key using bitwise XOR.

AES – Stage 2

Rounds

- SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
- ShiftRows - a transposition step where each row of the state is shifted cyclically a certain number of steps.
- MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey

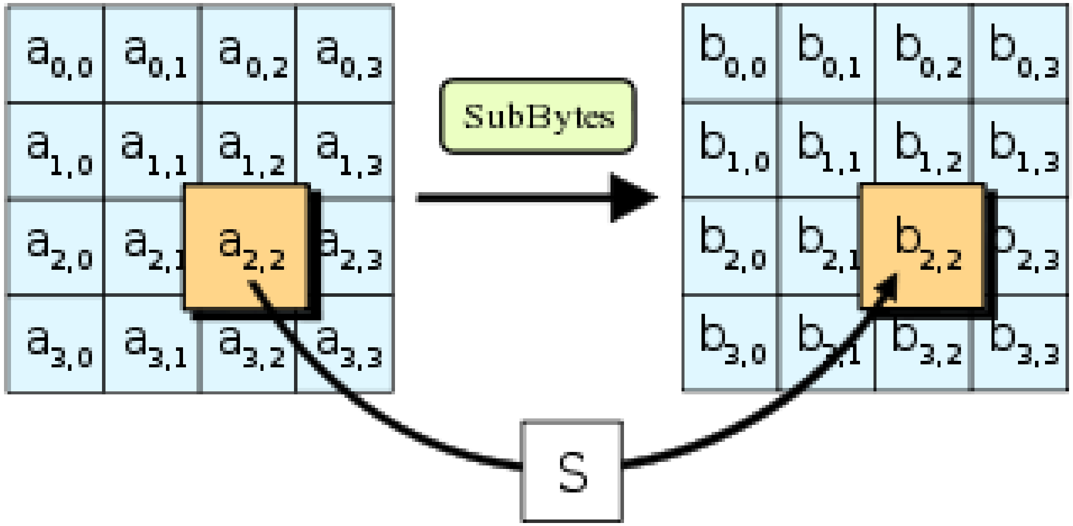
AES – Stage 3

Final Round (no MixColumns)

- SubBytes
- ShiftRows
- AddRoundKey

AES – SubBytes

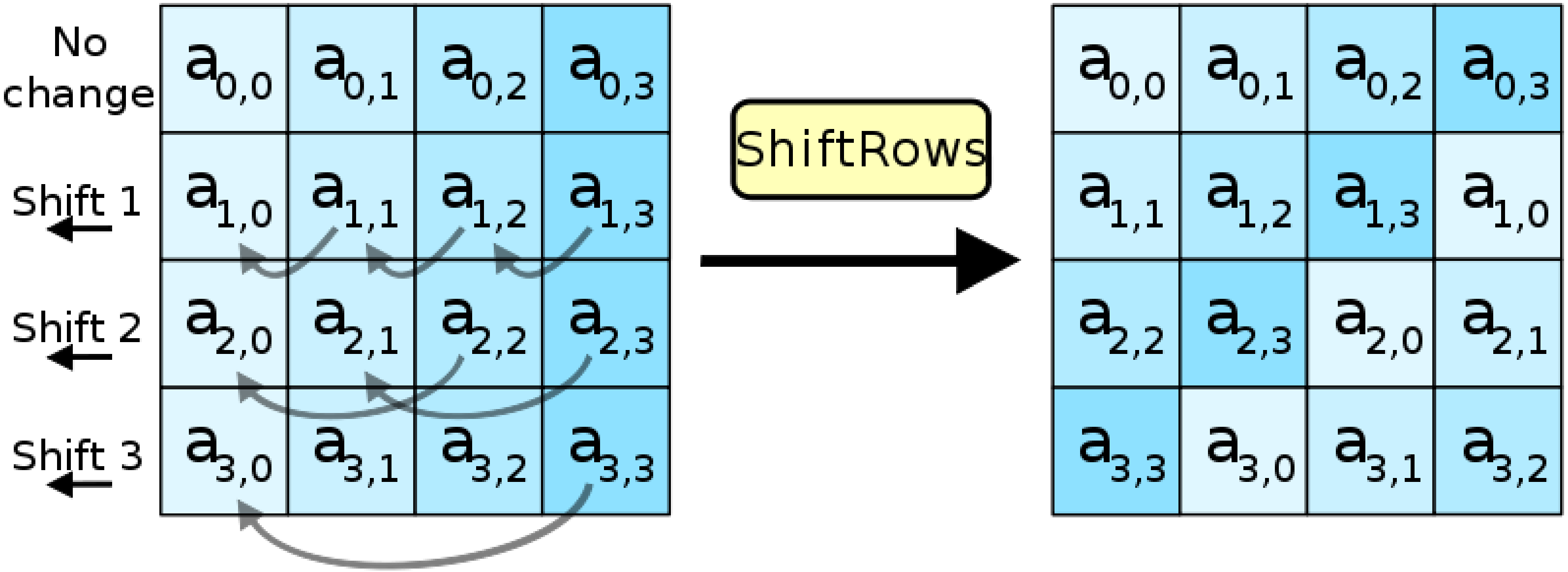
- Each byte is replaced with another based on a lookup table



$$\begin{array}{cccc} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{array} \xrightarrow{\text{SubBytes}} \begin{array}{cccc} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{array}$$

AES – ShiftRows

- A transposition step where each row of the state is shifted cyclically a certain number of steps

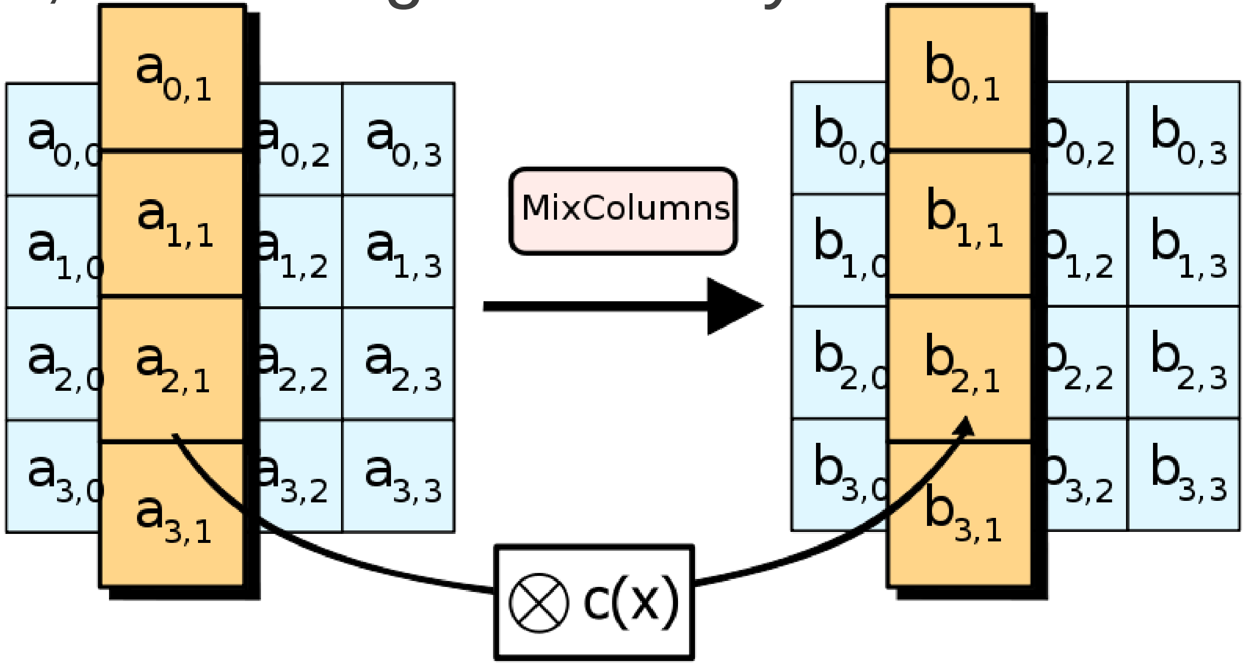


No change	$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
Shift 1	$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
Shift 2	$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
Shift 3	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,0}$
$a_{2,2}$	$a_{2,3}$	$a_{2,0}$	$a_{2,1}$
$a_{3,3}$	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$

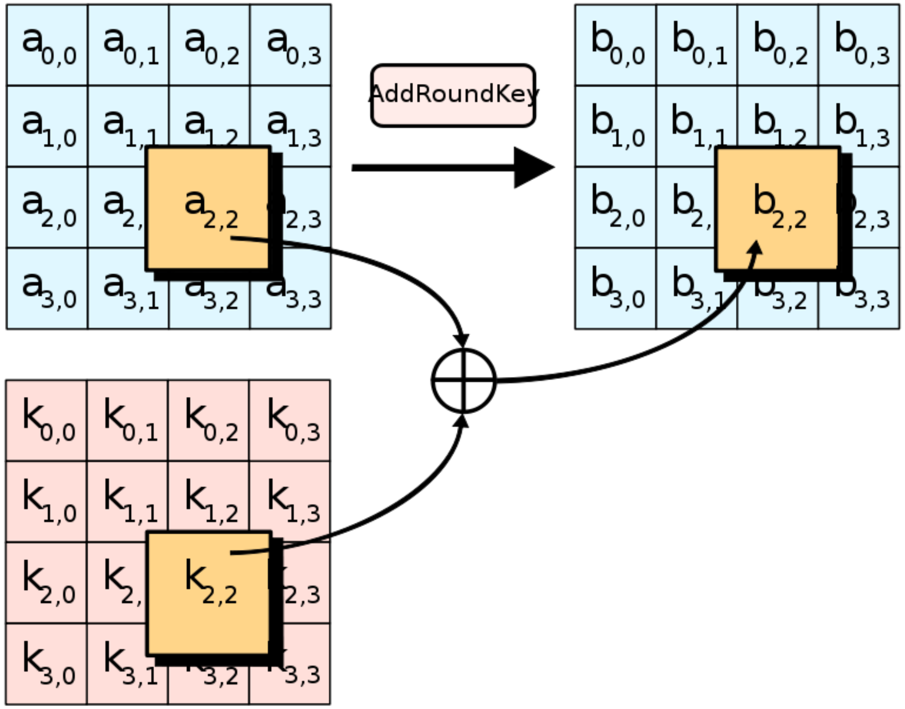
AES – MixColumns

- A mixing operation which operates on the columns of the state, combining the four bytes in each column


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$\otimes$ c(x)
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

AES – AddRoundKey

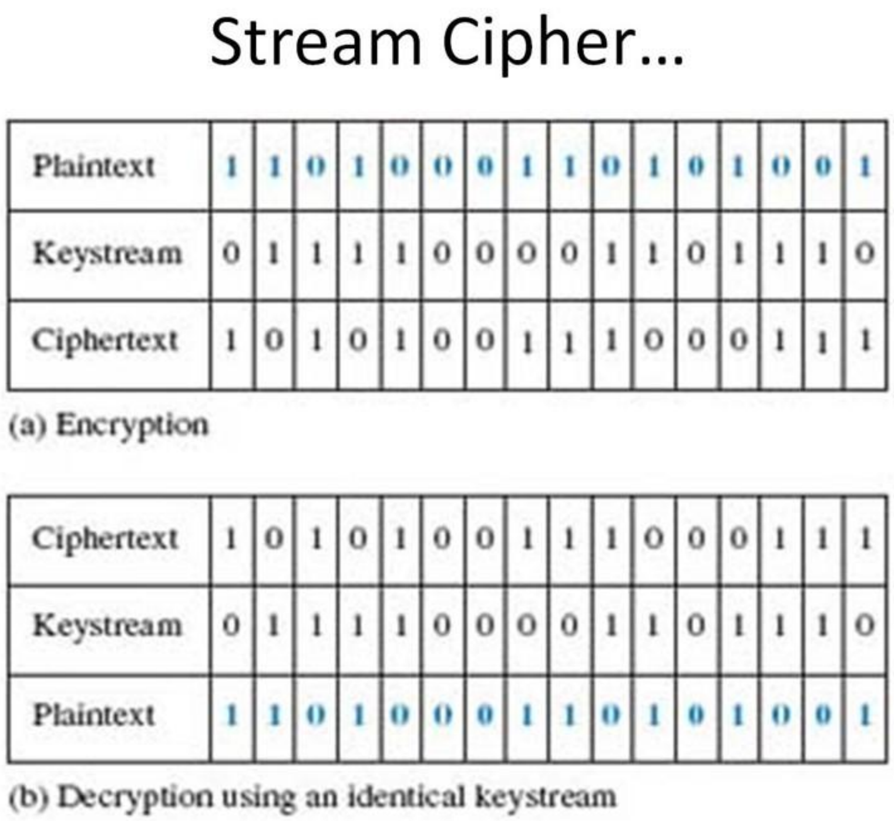
- Each byte of the state is combined with the round key using bitwise XOR


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
AddRoundKey
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$\oplus$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

Stream Cipher

- A stream cipher generally operates on one bit of plaintext at a time,
  - ✓ although some stream ciphers operate on bytes.
- A component called a keystream generator generates a sequence of bits, usually known as a keystream.
- In the simplest form of stream cipher, a modulo-2 adder (exclusive-OR) combines each bit in the plaintext with each bit in the keystream to produce the ciphertext.
- At the receiving end, another modulo-2 adder combines the ciphertext with the keystream to recover the plaintext.

Stream Cipher



Stream Cipher…

Plaintext	1	1	0	1	0	0	0	1	1	0	1	0	1	0	0	1
Keystream	0	1	1	1	1	0	0	0	0	1	1	0	1	1	1	0
Ciphertext	1	0	1	0	1	0	0	1	1	1	0	0	0	1	1	1

(a) Encryption

Ciphertext	1	0	1	0	1	0	0	1	1	1	0	0	0	1	1	1
Keystream	0	1	1	1	1	0	0	0	0	1	1	0	1	1	1	0
Plaintext	1	1	0	1	0	0	0	1	1	0	1	0	1	0	0	1

(b) Decryption using an identical keystream

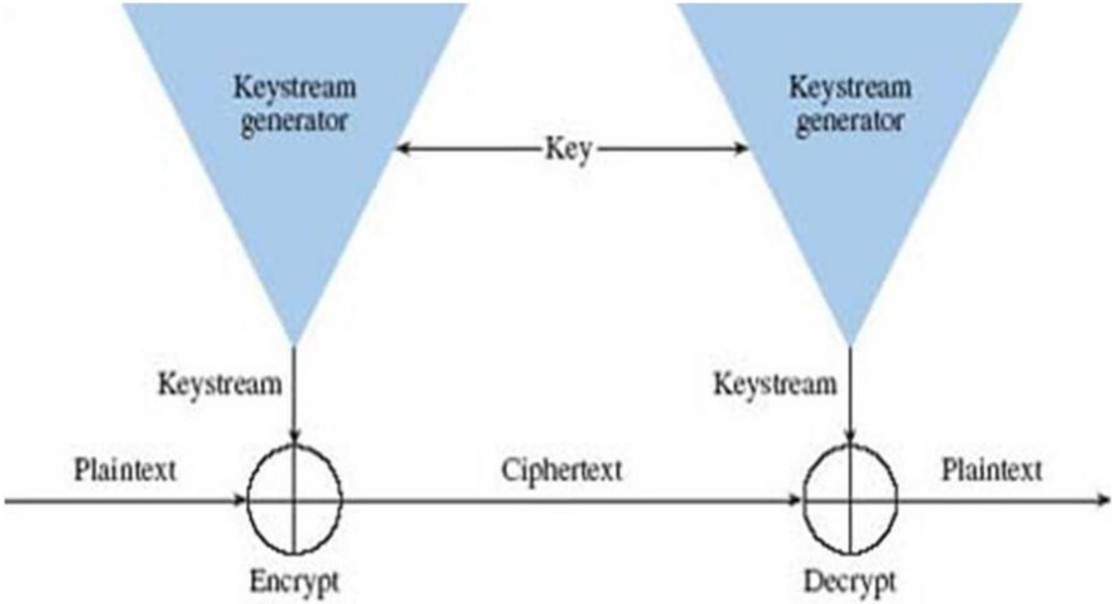
Stream Cipher

- Stream ciphers can be classified as either synchronous or self-synchronizing

- In a synchronous stream cipher, the **keystream** output is a function of a **key**, and is generated independently of the **plaintext** and the **ciphertext**.
  - ✓ A single bit error in the **ciphertext** will result in only a single bit error in the decrypted **plaintext**

Synchronous Stream Cipher

Synchronous stream cipher



Synchronous stream cipher (Source: based on Schneier, 1996, Figure 9.6)

Self-synchronizing Stream Cipher

- Key stream obtained from the secret key and N previous ciphertexts
- The receiver will automatically synchronize with the keystream generator after receiving N ciphertext digits, making it easier to recover if digits are dropped or added to the message stream.
- Lost packets cause a delay of q steps before decryption resumes
- Single-digit errors are limited in their effect, affecting only up to N plaintext digits.

Attacks on Stream Ciphers

Repetition attack

- if key stream reused, attacker obtains XOR of two plaintexts (why?)

Example of Stream Ciphers

RC4 (Rivest Cipher 4)

- RC4 is one of the most well-known stream ciphers and was designed by Ronald Rivest in 1987.
- It is widely used in various cryptographic protocols and applications, including Wi-Fi encryption (WEP and WPA), SSL/TLS, and secure communication systems.
- RC4 operates on a variable-length key (ranging from 1 to 256 bytes) and generates a pseudo-random key stream that is XORed with the plaintext to produce the ciphertext.
- The keystream generation in RC4 is based on a combination of permutation and substitution operations on a 256-byte state array.
- However, due to certain vulnerabilities and biases in its initial key states, RC4 is no longer considered secure for modern cryptographic applications, and its usage is strongly discouraged.

Example of Stream Ciphers

Salsa20

- Salsa20 is a family of stream ciphers designed by Daniel J. Bernstein in 2005.
- It is known for its simplicity, high performance, and strong security properties, making it a popular choice in various applications, including disk encryption, VPN protocols, and secure messaging.
- Salsa20 operates on a 256-bit secret key and a 64-bit initialization vector (IV).
- The keystream generation in Salsa20 uses a series of fast and simple operations, including bitwise addition, rotation, and modular addition.
- The design of Salsa20 aims to provide excellent security and resistance to cryptanalysis, making it suitable for use in modern cryptographic systems.

Block vs Stream Cipher

Aspect	Block Cipher	Stream Cipher
Mode of Operation	Encrypt fixed-sized blocks of data	Encrypt data one bit or byte at a time
Speed	Typically, slower for short messages	Generally faster for real-time applications
Key Management	Need key expansion for each block	Easier key management, ideal for constrained environments
Security	Provide strong security when used properly	Susceptible to certain attacks if not designed carefully
Use Cases	Suitable for data at rest, like file encryption	Ideal for real-time communication and data streaming
Examples	AES, DES, 3DES	RC4, A5/1, Salsa20

Topic Summary

- Symmetric Cryptography: single secret key between the two communicating entities.
- Classical ciphers primarily rely on simple substitution and transposition techniques.
- Modern ciphers are based on mathematic and classified as block and stream ciphers.
- Block ciphers use algorithms to encrypt and decrypt a fixed-size block of plaintext and ciphertext, respectively, usually a multiple of 64 bits.

Topic Summary

- Stream ciphers continuously encrypt any amount of data as it is presented, usually by mathematically combining the data with a keystream, an infinitely long key sequence that is generated based on a finite key starting value.
- The key length is crucial in cryptography as longer keys increase the resistance to attack, making it significantly more challenging for adversaries to decrypt encrypted data.
- However, sharing a secret key between two parties over an insecure communication channel is the fundamental issue in these algorithms.

Next Topic 3: Cryptographic Techniques

- Asymmetric Key Cryptography
- Hash Function/digital signatures
- Message Authentication Code

References

- CHARLES J. B., Christopher G., Philip C., Donald S. 2018. Cybersecurity Essentials, John Wiley & Sons, Inc.
- CIAMPA, M. (2012). Security+ guide to network security fundamentals. Cengage Learning.
- HOFFMAN, A. 2020. Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly.
- OZKAYA, E. 2019. Cybersecurity: The Beginner's Guide. Packet Publishing Ltd.
- STALLINGS, W. 2022. Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition, Pearson.

NCC education®

Awarding
Great British
Qualifications

Topic 2 – Cryptographic Techniques

Any Questions?