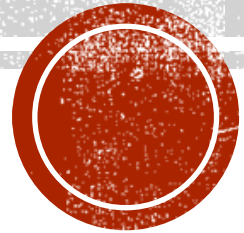
LECTURE 6

Information Security 2024

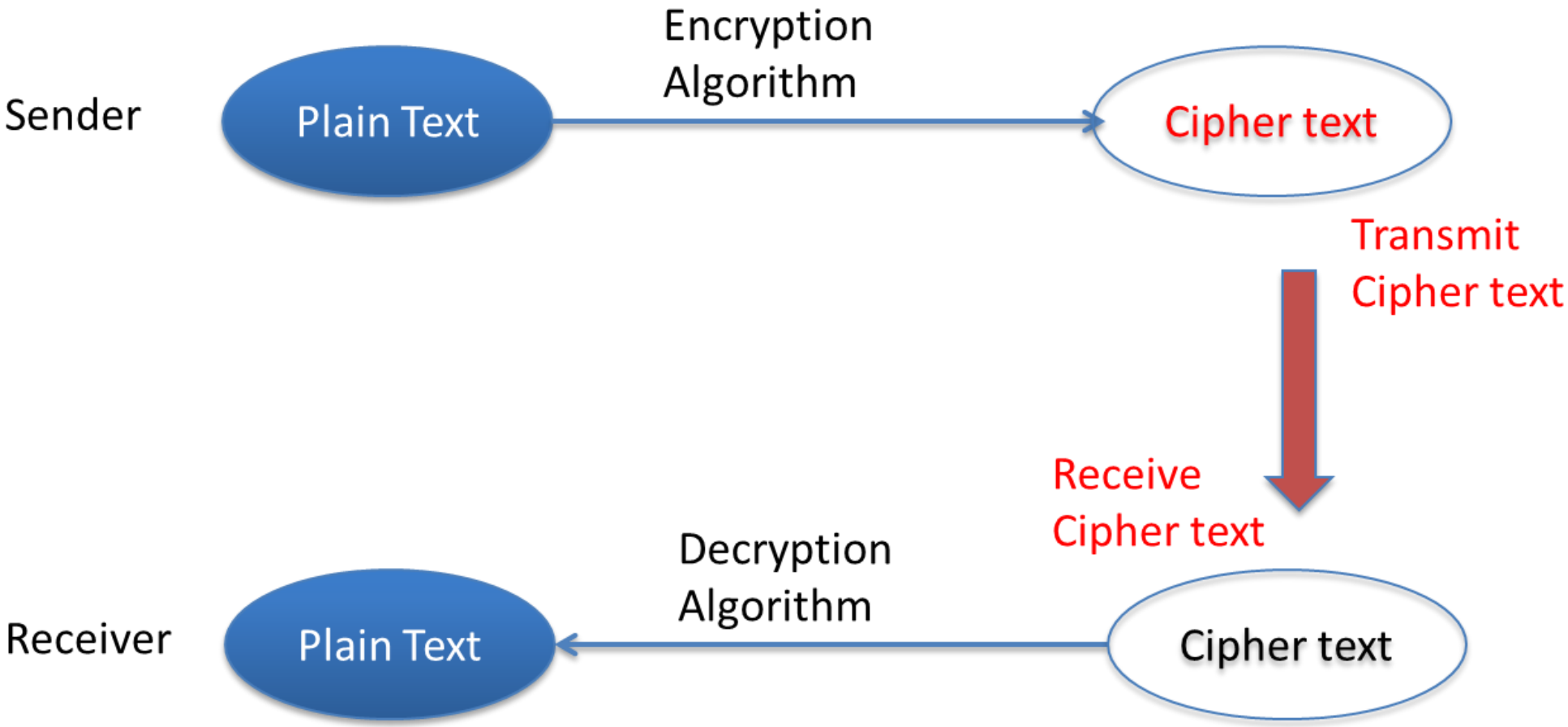
Topic: Modern Cryptography



AGENDA

- Quiz
- Block Cipher
- Stream Cipher
- DES
- 3DES
- AES
- Hashing
- Cracking passwords

Cryptography Concept



Q1

- Betty receives a cipher text message from her colleague Tim. What type of function does Betty need to use to read the plaintext message?
- Encryption
- Hashing
- Decryption
- Validation

Q2

- Which of the following is an encryption key of assymetric system?
- Public
- Private
- Both a and b
- Zero key

Q3

- In the Caesar cipher, if 'A' is shifted three places, it becomes
- D
- C
- B
- E

CLASSIC VS MODERN

Classic Cryptography

- It manipulates traditional characters, i.e., letters and digits directly.
- It is mainly based on 'security through obscurity'. The techniques employed for coding are kept secret and only the parties involved in communication knew about them.

Modern Cryptography

- It operates on binary bit sequences.
- It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secrete key which is used as the seed for the algorithms.

Tutorialspoint, 2023

MODERN CRYPTO

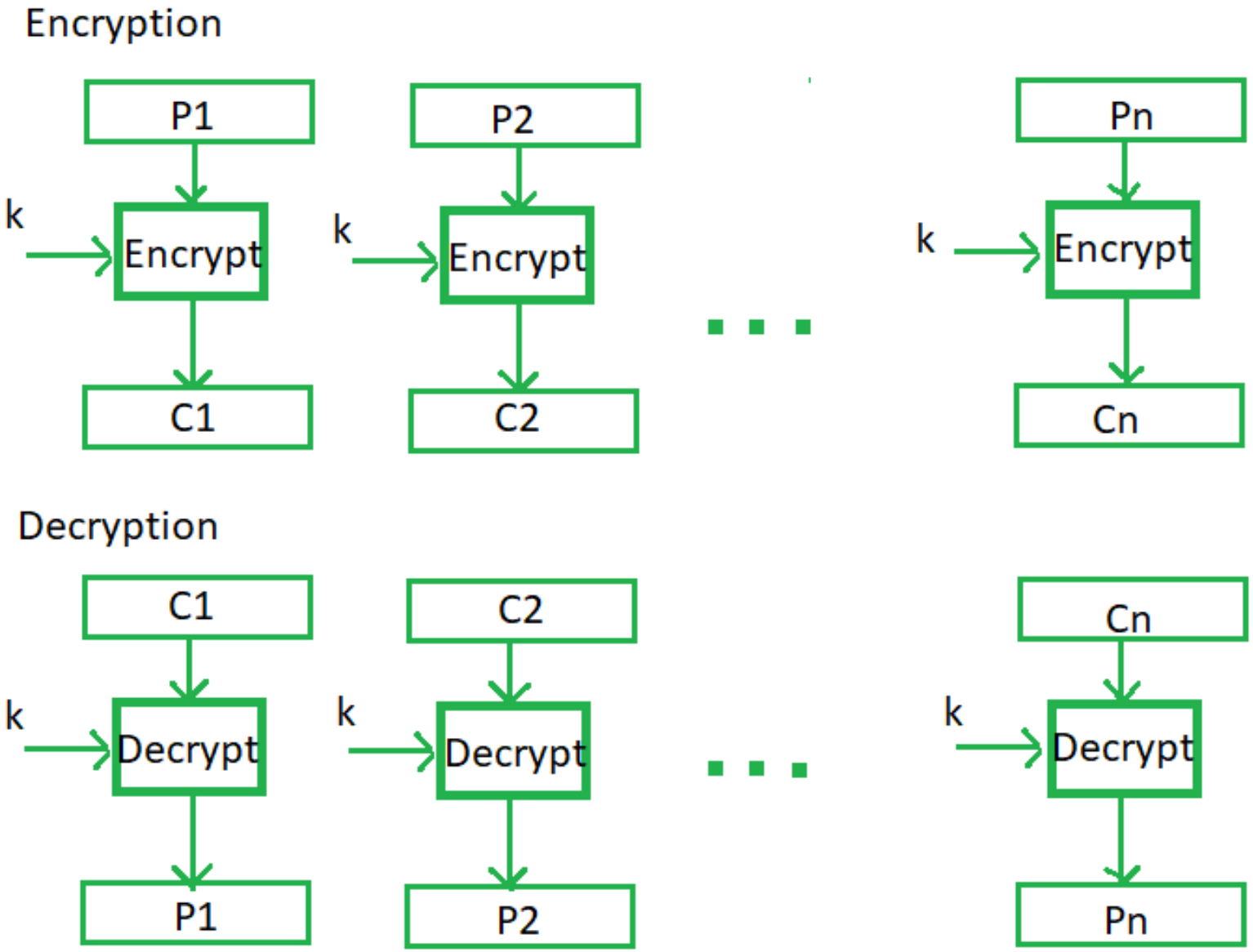
- Modern symmetric ciphers can be subdivided into **stream ciphers and block ciphers.**
- Today, **block ciphers** are the kings of the symmetric crypto world
- **Block ciphers** are easier to optimize for software implementations
- **Stream ciphers** are usually most efficient in hardware

BLOCK VS STREAM

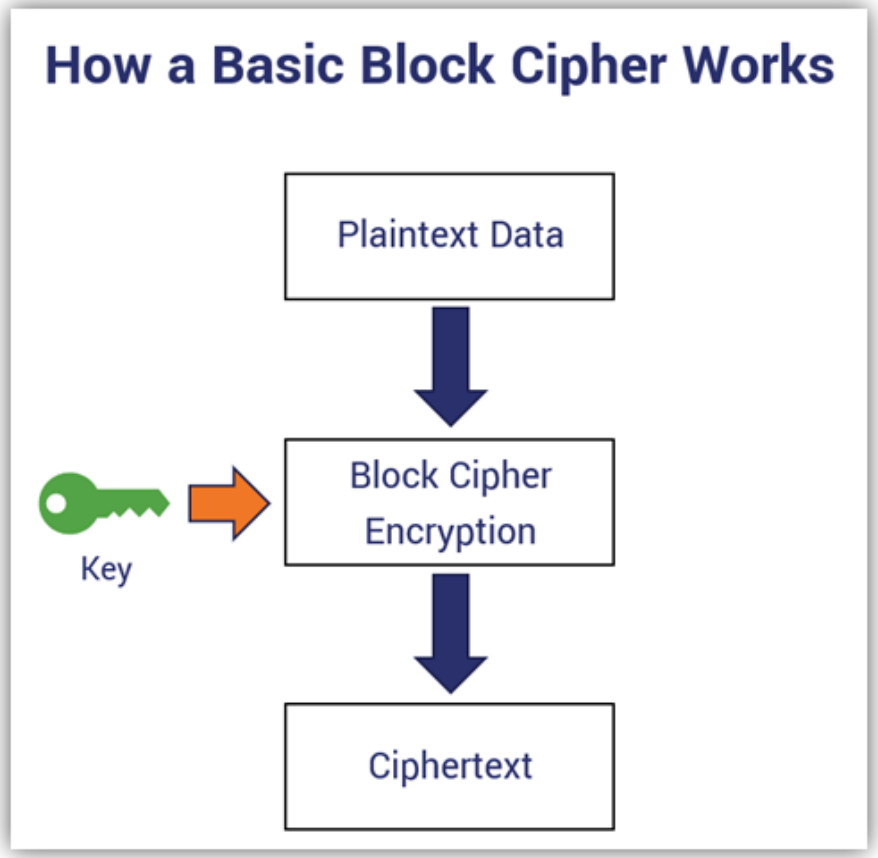
- The big difference between the two is how the data gets encrypted
- There are advantages and disadvantages to each method
- Block Cipher- Encrypting information in chunks. A block ***cipher breaks down plaintext messages into fixed-size blocks*** before converting them into ciphertext using a key.
- Stream Cipher- A stream cipher, on the other hand, breaks a plaintext message down into single bits, which then are converted individually into ciphertext using key bits.

BLOCK CIPHERS

- A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
- Typically, a **block size of 64 or 128 bits is used.**
- So for example, a 64-bit block cipher will take in 64 bits of plaintext and encrypt it into 64 bits of ciphertext.


Encryption
P1
k
Encrypt
C1
P2
k
Encrypt
C2
Pn
k
Encrypt
Cn
Decryption
C1
k
Decrypt
P1
C2
k
Decrypt
P2
Cn
k
Decrypt
Pn

BLOCK CIPHER



BLOCK CIPHER

- Suppose we have the message: "THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG".
- In Binary:
- 01010100 01001000 01000101 00100000 01010001 01010101 01001001 01000011
- 01001011 00100000 01000010 01010010 01001111 01010111 01001110 00100000
- 01000110 01001111 01011000 00100000 01001010 01010101 01001101 01010000
- 01010011 00100000 01001111 01010110 01000101 01010010 00100000 01010100
- 01001000 01000101 00100000 01001100 01000001 01011010 01011001 00100000
- 01000100 01001111 01000111

- Block 1: 01010100 01001000 01000101 00100000 01010001 01010101 01001001 01000011
- (T H E [space] Q U I C)

- Block 2: 01001011 00100000 01000010 01010010 01001111 01010111 01001110 00100000
- (K [space] B R O W N [space])

- Block 3: 01000110 01001111 01011000 00100000 01001010 01010101 01001101 01010000
- (F O X [space] J U M P)

- Block 4: 01010011 00100000 01001111 01010110 01000101 01010010 00100000 01010100
- (S [space] O V E R [space] T)

- Block 5: 01001000 01000101 00100000 01001100 01000001 01011010 01011001 00100000
- (H E [space] L A Z Y [space])

- Block 6: 01000100 01001111 01000111 00000000 00000000 00000000 00000000 00000000
- (D O G)

EXAMPLES OF BLOCK CIPHERS

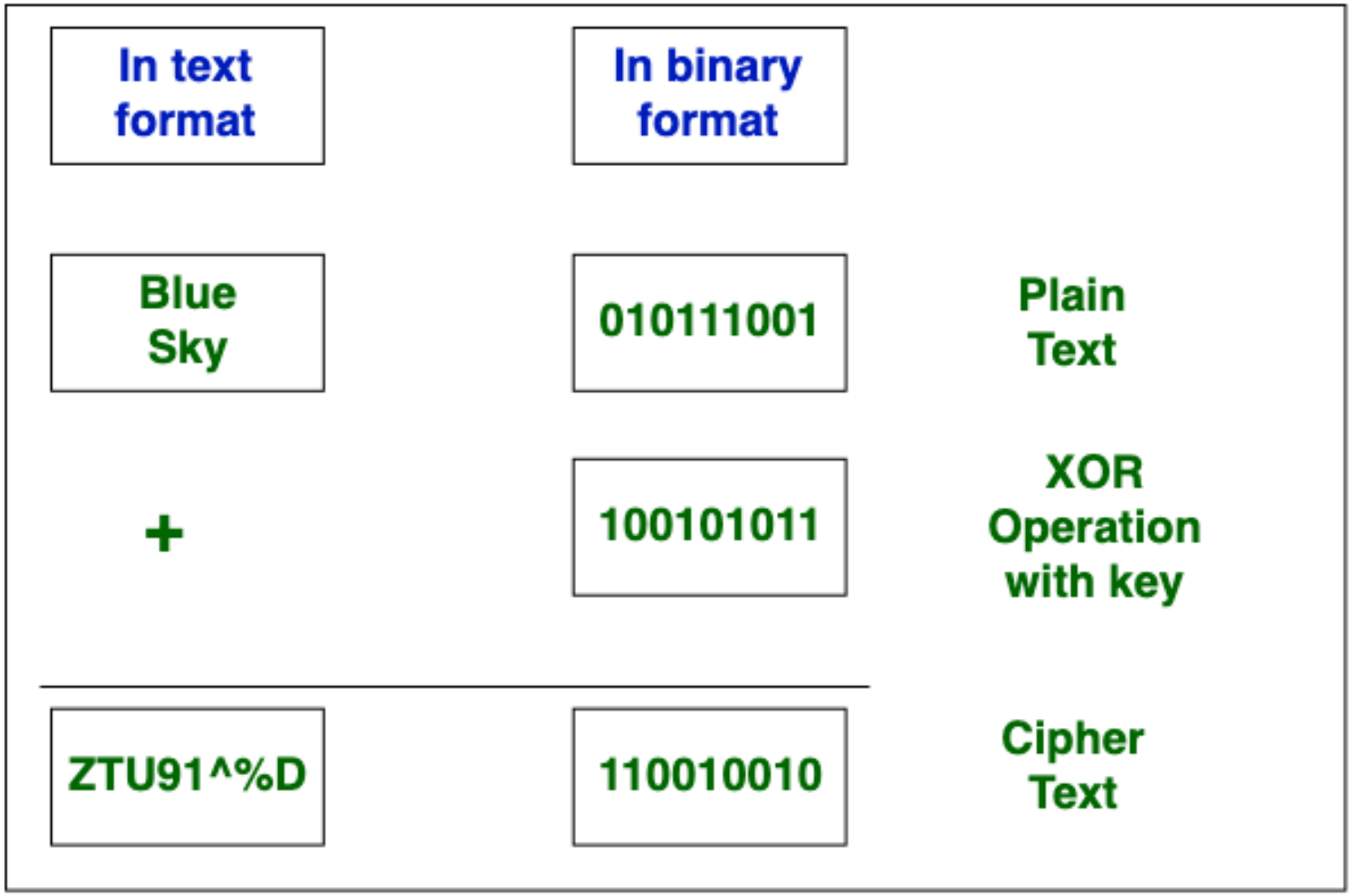
- Data Encryption Standard (DES),
- Triple DES ,
- Advanced Encryption Standard (AES),
- International Data Encryption Algorithm (IDEA),
- Blowfish,
- Twofish, and
- RC5

STREAM CIPHER

- Encrypts (and decrypts) with the flow — the data flow, that is.
- Unlike block ciphers, which require the formation of blocks prior to encryption, stream ciphers encrypt data in long, pseudorandom streams.
- Stream algorithms are faster, because they're encrypting only one bit of data at a time into individual symbols rather than entire blocks.
- Better suited for devices that have fewer resources.

STREAM CIPHERS

- In a stream cipher, the plaintext is combined with a keystream (a sequence of pseudorandom or truly random values) to produce the ciphertext.
- The keystream is typically generated based on a cryptographic key and is XORed with the plaintext to produce the ciphertext.
- Security depends on key management and key exchange
- If the keystream is predictable or reused, it can lead to cryptographic vulnerabilities



Stream Cipher

STEAM CIPHER

- Plaintext: H E L L O
- 01001000 01000101 01001100 01001100 01001111
- Keystream: 10101010 10101010 10101010 10101010 10101010
- Ciphertext: 11100010 11101111 11100110 11100110 11100101

EXAMPLES OF STREAM CIPHER

- RC4 algorithm, - widely used in various applications, including SSL/TLS protocols, but its usage has declined due to security vulnerabilities
- Salsa20/ChaCha – VPN, Disk Encryption, Tor (The Onion Router)
- A5/1 and A5/2 - used in GSM (Global System for Mobile Communications) cellular networks for voice encryption, 4G, 5G
- E0 (Bluetooth Encryption)
- Rabbit – e.g in disk encryption

FEISTEL CIPHER

- Symmetric structure used in block ciphers
- Developed by German-born physicist and cryptographer **Horst Feistel**
- IBM
- Known as fiestel network

FEISTEL CIPHER STRUCTURE

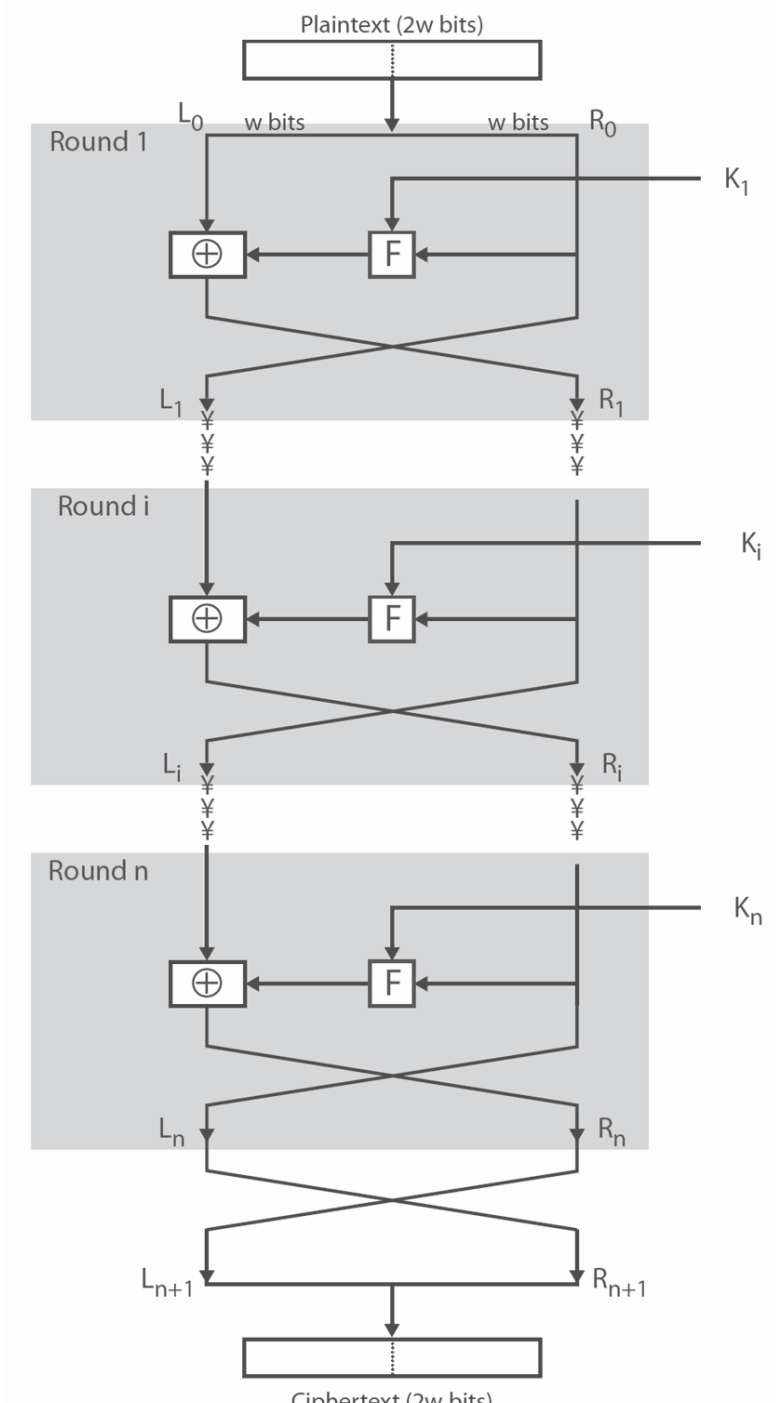
Most symmetric block ciphers are based on a **Feistel Cipher Structure.** For defining the complexity level of an algorithm few design principles are to be considered.

1. Number of Rounds
2. Design of function F
3. Key schedule algorithm

FEISTEL CIPHER PRINCIPLES

1. Block Division- The input block of plaintext is divided into two equal halves.
2. Round Function- The Feistel cipher iterates through a series of rounds, each consisting of a round function.
3. Key Schedule- In each round, a subkey derived from the main encryption key is used
4. Iteration: The Feistel cipher iterates through multiple rounds, typically 16 rounds for many modern block ciphers. Each round uses a different round key generated from the main encryption key.
5. Reversibility: The Feistel cipher is reversible. To decrypt the ciphertext, the same algorithm is applied, but the round keys are used in the reverse order.
6. Final Permutation: After all rounds have been completed, a final permutation is applied to the block to ensure that the final output does not directly resemble the original plaintext.

FEISTEL CIPHER STRUCTURE



FEISTEL CIPHER DESIGN ELEMENTS

- block size
- key size
- number of rounds
- subkey generation algorithm
- round function
- fast software en/decryption
- ease of analysis

DES/AES

- DES (Data Encryption Standard) and AES (Advanced Encryption Standard) both are **the symmetric block cipher.**
- AES was introduced to overcome the drawback of DES
- As DES has a smaller key size which makes it less secure to overcome this, **3 DES** was introduced but it turns out to be **slower.**
- Hence, later AES was introduced by the National Institute of Standard and Technology (NIST).

DATA ENCRYPTION STANDARD (DES)

- most widely used block cipher in world
- DES is Feistel cipher with the following numerology:

1. 16 rounds
2. 64-bit block length
3. 56-bit key
4. 48-bit subkeys

- adopted in 1977 by NBS (now NIST)
- encrypts 64-bit data using 56-bit key
- has been considerable controversy over its security

DES DESIGN CONTROVERSY

- although DES standard is public
- was considerable controversy over design
  - in choice of 56-bit key (vs Lucifer 128-bit)
- subsequent events and public analysis show in fact design was appropriate
- use of DES has flourished
  - especially in financial applications
  - still standardised for legacy application use

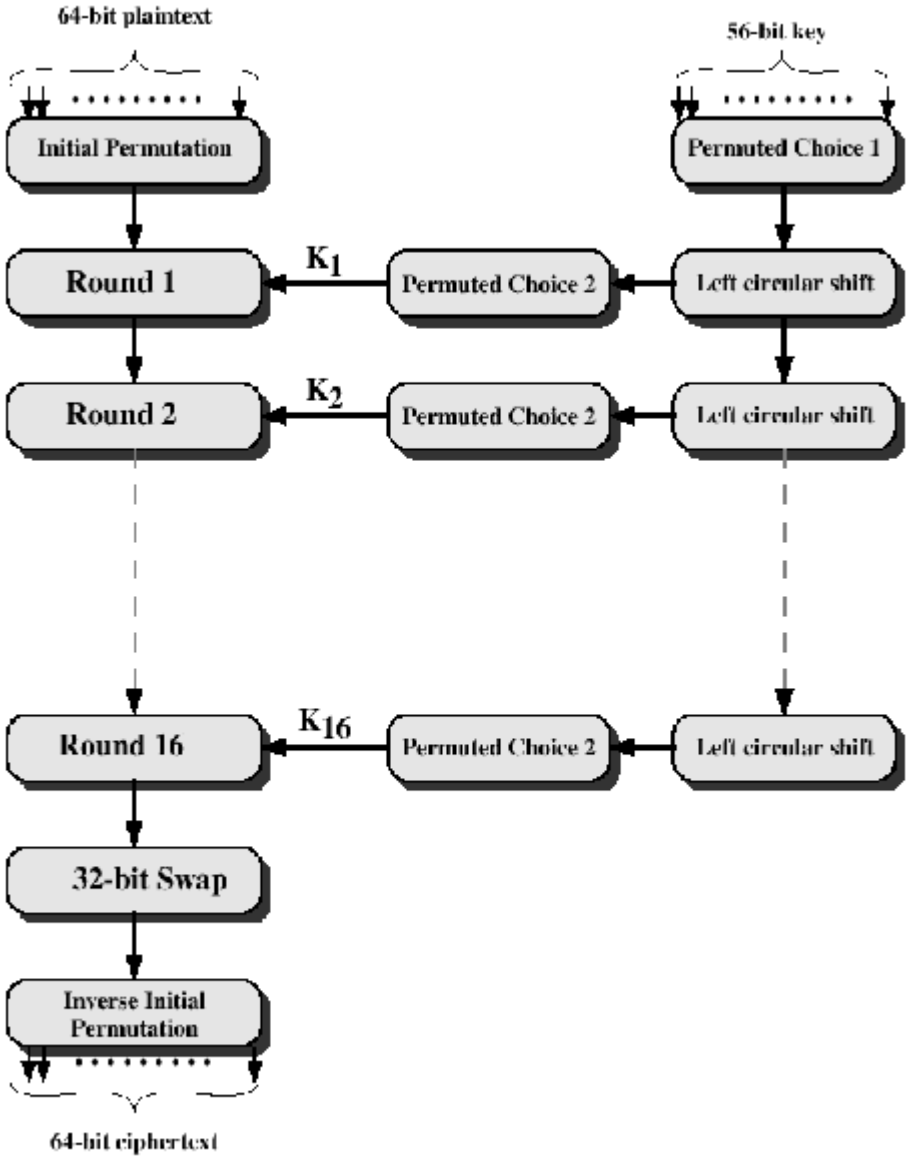


Figure 2.3 General Depiction of DES Encryption Algorithm

DES...

- **Initial Permutation (IP):**

>The plaintext block undergoes an intial permutation.

>64 bits of the block are permuted.

> provide some diffusion and confusion in the plaintext before it goes through the main encryption rounds

The Initial Permutation: IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP EXAMPLE

- Input (plaintext):

01110010 11001100 00111100 10101010 01010101 11100000 00011110 11000011

- Output (after initial permutation):

00100111 10010110 01111000 00100011 01100110 00101011 11001000 00011111

DES

- **A Complex Transformation:**
- 64 bit permuted block undergoes 16 rounds of complex transformation. (Using subkeys)

DES...

- **32-bit swap:**

  32 bit left and right halves of the output of the 16th round are swapped.

- **Inverse Initial Permutation (IP-1):**

  The 64 bit output undergoes a permutation that is inverse of the intial permutation.

>The 64 bit output is the ciphertext.

Initial and final permutation tables

Initial Permutation								*Final Permutation*							
58	50	42	34	26	18	10	02	40	08	48	16	56	24	64	32
60	52	44	36	28	20	12	04	39	07	47	15	55	23	63	31
62	54	46	38	30	22	14	06	38	06	46	14	54	22	62	30
64	56	48	40	32	24	16	08	37	05	45	13	53	21	61	29
57	49	41	33	25	17	09	01	36	04	44	12	52	20	60	28
59	51	43	35	27	19	11	03	35	03	43	11	51	19	59	27
61	53	45	37	29	21	13	05	34	02	42	10	50	18	58	26
63	55	47	39	31	23	15	07	33	01	41	09	49	17	57	25

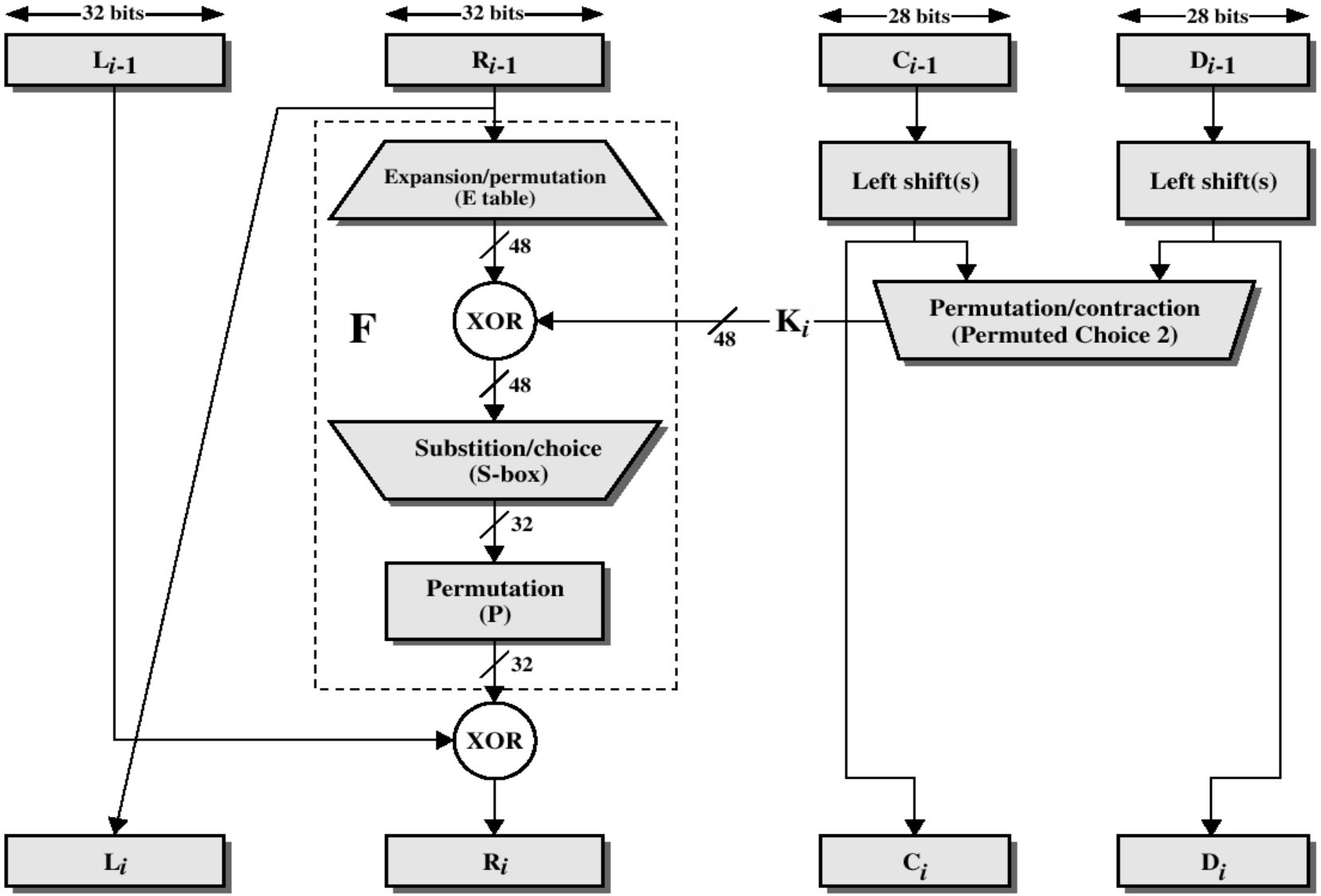


Figure 2.4 Single Round of DES Algorithm

DES

- **The complex processing at each iteration/round:**
  - Li = Ri-1
  - Ri = Li-1 $\otimes$ F(Ri-1, Ki)
- **Details of function F:**

  It takes 32 bits input and produces a 32 bit output.

DES

- **Details of function F:**

  >32 bit input is expanded into 48 bits.

  -This is done by permuting and duplicating some bits of 32 bits.

  >Exclusive OR operation is performed between these 48 bits and 48 bit subkey.

DES Expansion Permutation

- Input 32 bits

```
 0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
```

- Output 48 bits

```
31  0  1  2  3  4  3  4  5  6  7  8
 7  8  9 10 11 12 11 12 13 14 15 16
15 16 17 18 19 20 19 20 21 22 23 24
23 24 25 26 27 28 27 28 29 30 31  0
```


DES

- **Details of function F:...**

  > 48 bit output of the Exclusive OR operation is grouped into 8 groups of 6 bits each.

  > Each 6 bit group is fed into a 6-to-4 substitution box that transforms 6 bits to 4 bits.

DES

- **Details of function F:...**

  > 32 bit output of 8 substitution boxes is fed into a permutation box.

  > The 32 bit output of the permutation box is F(Ri-1, Ki).

DES

- **Concerns about:**
  - The key length (56-bits)
  - > 56 bit key was adequate in 70s.
  - > With faster processors, this encryption method is no longer safe.

BRUTE FORCE

- Generate all possible 56-bit keys. Since each key bit has two possible values (0 or 1), there are **2^56** possible keys
- For each generated key, encrypt the plaintext using DES with that key.
- Compare with Ciphertext: Compare the resulting ciphertext with the known ciphertext. If the ciphertext matches the known ciphertext, the correct key has been found.

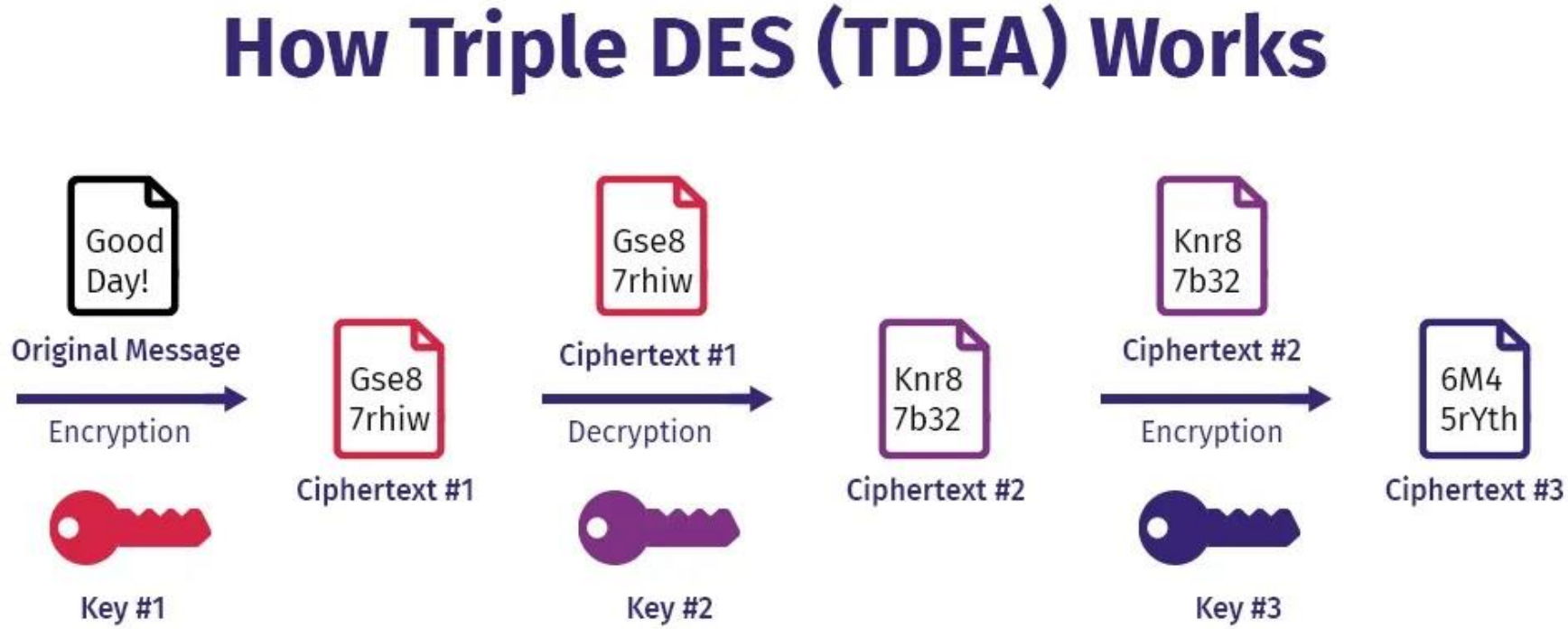
BRUTE FORCE

Chronology of DES Cracking	
Broken for the first time	1997
Broken in 56 hours	1998
Broken in 22 hours and 15 minutes	1999
Capable of broken in 5 minutes	2021

Source: Wikipedia

3DES

- Triple DES encrypts input data three times. The three keys are referred to as k1, k2, and k3
- In 1990s



3DES

- The encryption process of 3DES involves the following steps:
- ***Key Generation:*** *Three unique keys are generated using a key derivation algorithm.*
- ***Initial Permutation:*** *The 64-bit plaintext is subjected to an initial permutation.*
- ***Three Rounds of Encryption:*** *The plaintext is encrypted three times, each time using a different key, to create three layers of encryption.*
- ***Final Permutation:*** *After the three rounds of encryption, a final permutation is applied to the output to produce the ciphertext.*
- (Nagaraj, 2023)

LIMITATIONS (3DES)

- Limitations of 3DES
- **Slow Speed**: The triple-layered encryption process of 3DES makes it slower than other encryption algorithms.
- **Limited Key Size Options**: While 3DES supports variable key sizes, the maximum key size is only 192 bits, which may not be enough to meet the security needs of some applications.

HERE COMES AES

- Advanced Encryption Standard
- In 2001 by National Institute of Standards and Technology
- AES algorithm takes 128-bit plaintext and 128-bit secret key which together forms a 128-bit block which is depicted as 4 X 4 square matrix.

AES VS DES

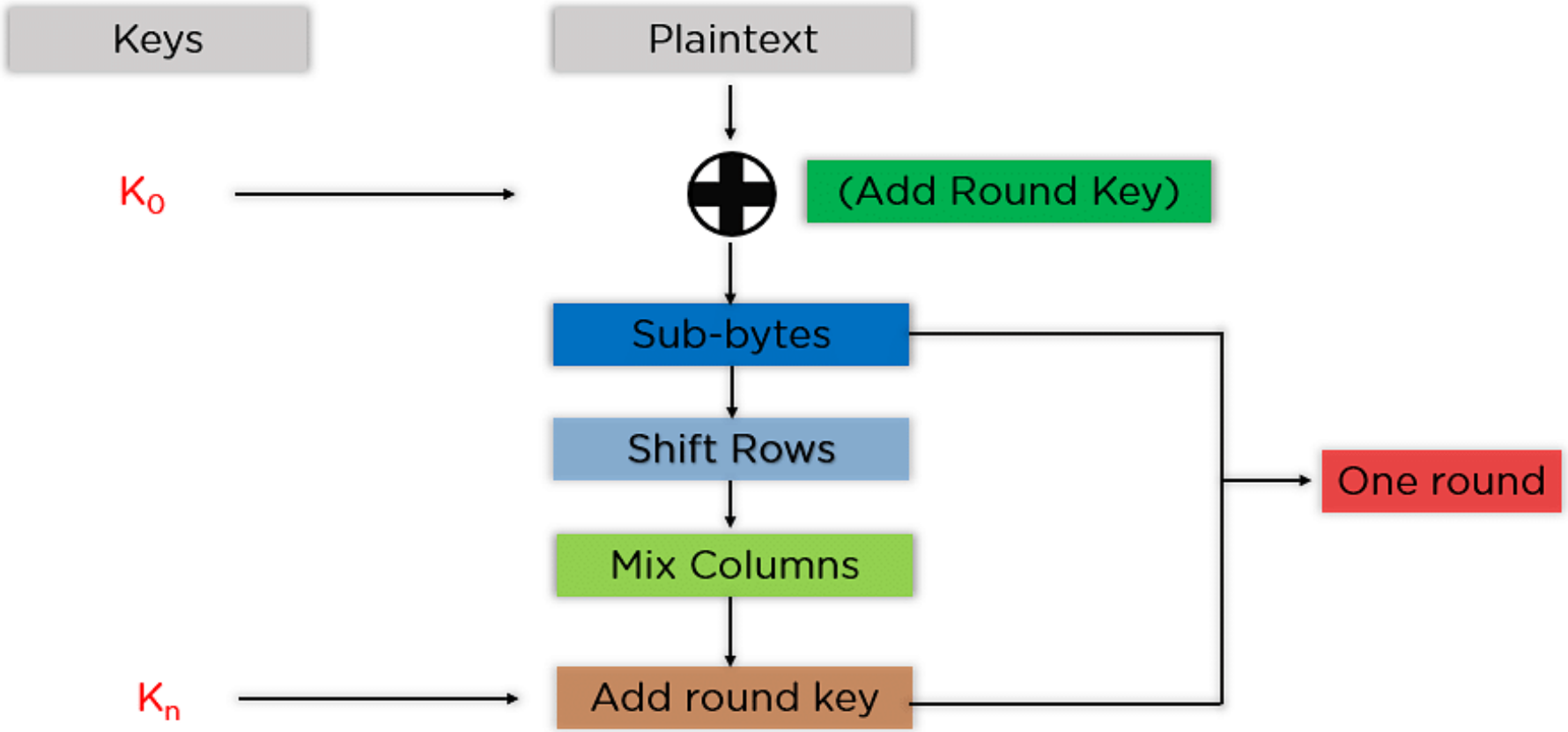
- The basic difference between DES and AES is >
- in DES plaintext block is divided into two halves before the main algorithm starts whereas, in AES the entire block is processed to obtain the ciphertext.
- In DES, the plaintext is 64 bits
- In AES, plaintext can be of **128, 192, or 256 bits**
- DES has smaller key size than AES

AES

- he AES encryption algorithm does operations on byte data instead of bit data.
- So it treats the 128-bit block size as 16 bytes during the encryption procedure.

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

AES


Keys
Plaintext
K_0
(Add Round Key)
Sub-bytes
Shift Rows
Mix Columns
Add round key
K_n
One round

SHIFT ROWS

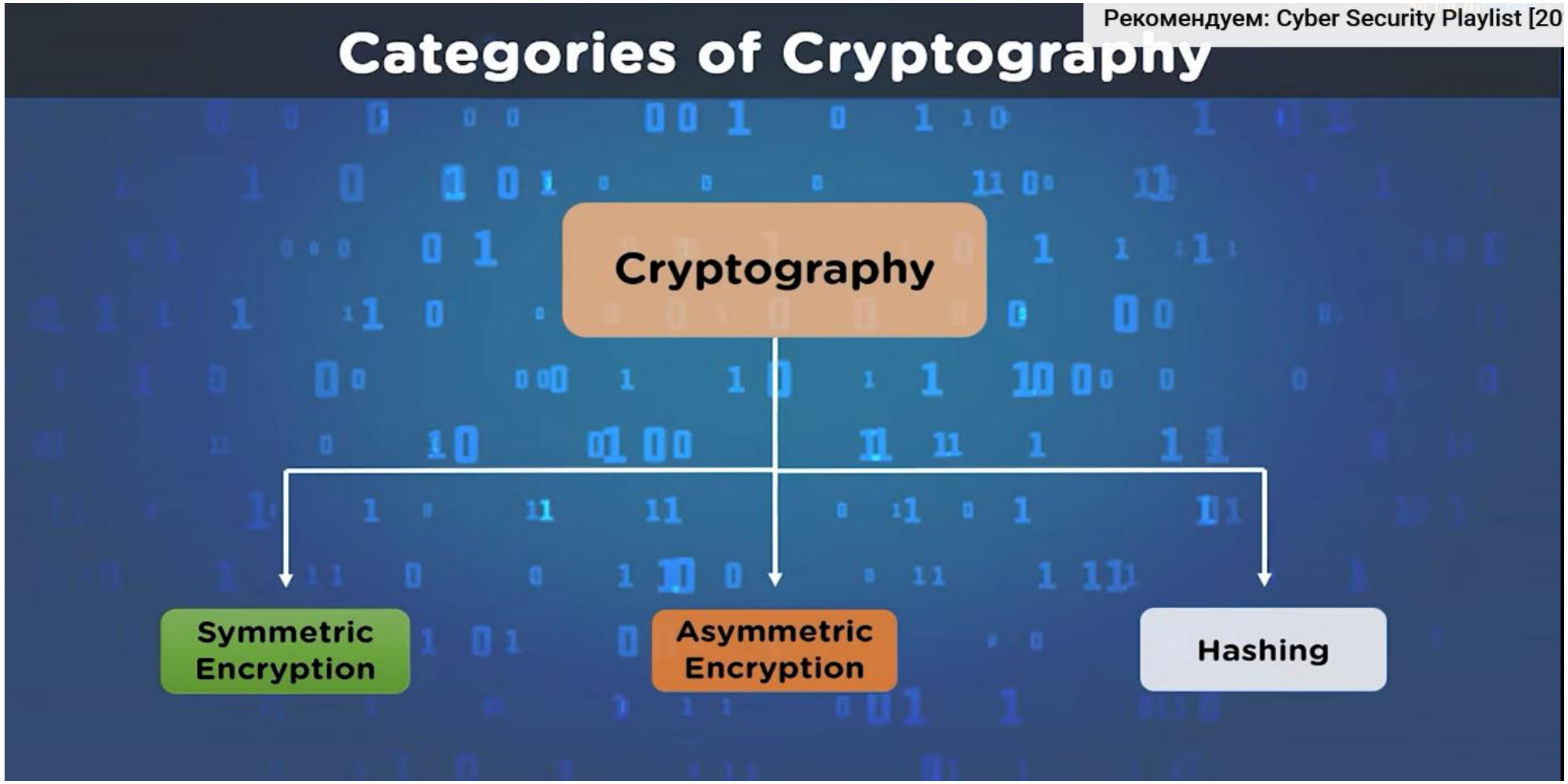
- Original State Matrix:
- S0 S4 S8 S12
- S1 S5 S9 S13
- S2 S6 S10 S14
- S3 S7 S11 S15

- After ShiftRows:
- S0 S4 S8 S12
- S5 S9 S13 S1
- S10 S14 S2 S6
- S15 S3 S7 S11

APPLICATIONS

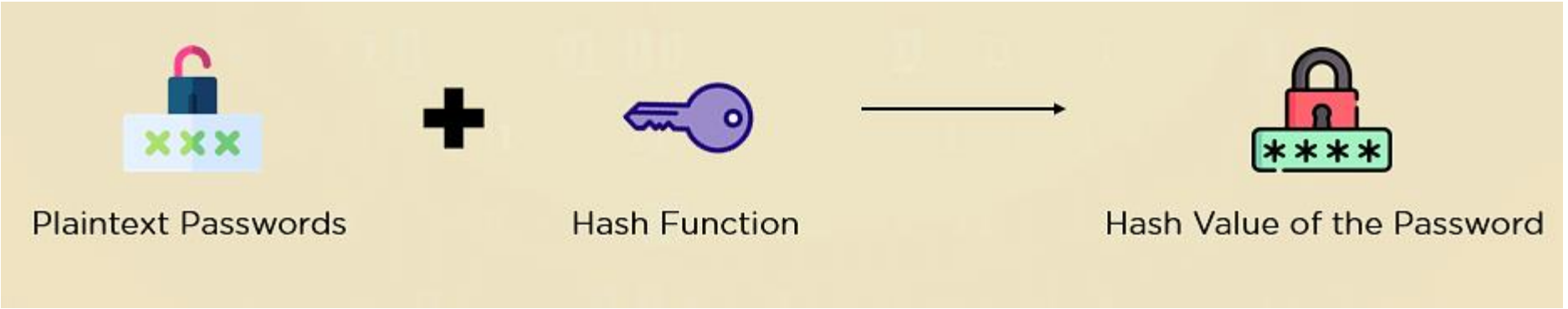
- Wireless security
- Encrypted browsing
- General file encryption
- Secure messaging, chat applications
- Payment Card Industry

Рекомендуем: Cyber Security Playlist [20



HASHING

- Involves taking the plain text and converting it to a hash value of fixed size by a hash function
- Scrambles data beyond recognition
- However, unlike symmetric and asymmetric key cryptography, hashing isn't designed to be reversible



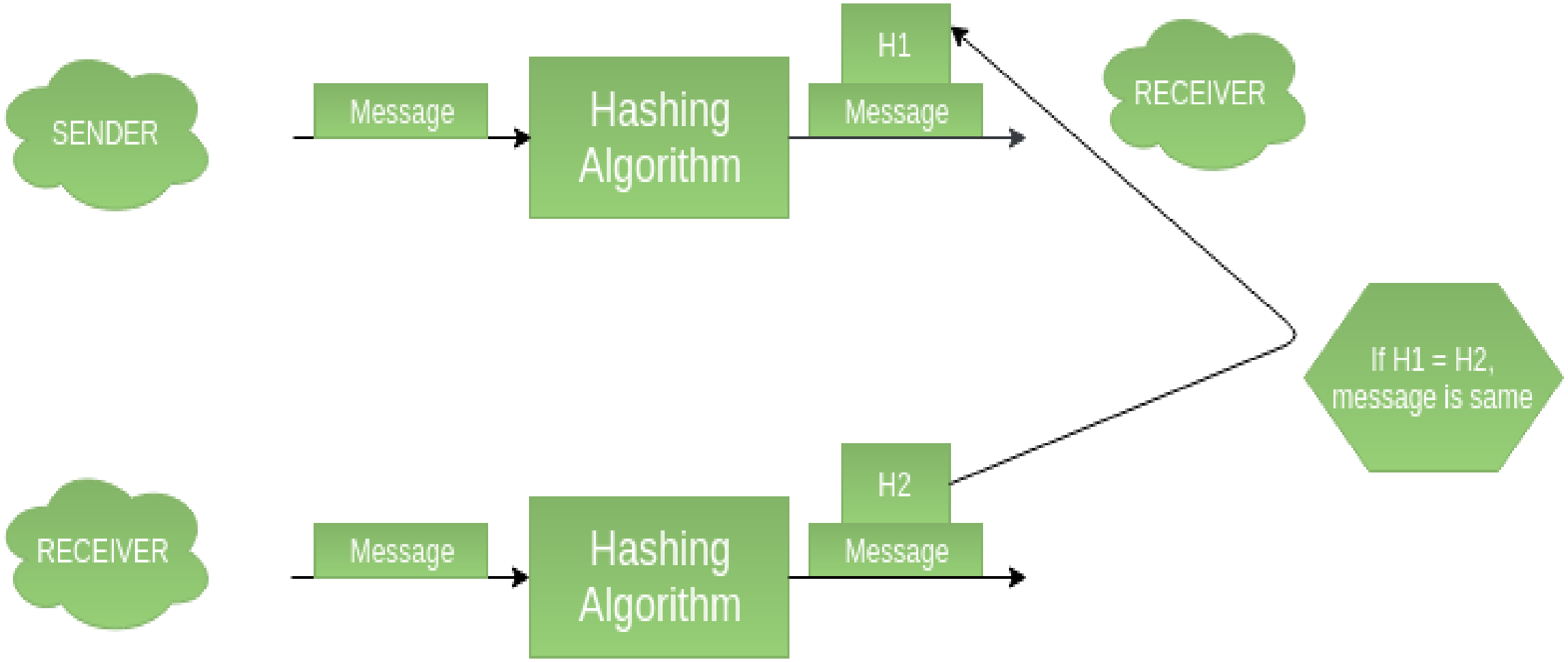
WHY IMPORTANT

- Sometimes, you want to be able to store and retrieve sensitive information.
- For example, many websites don't store your actual password in a database but rather your password's hash value instead.
- Especially useful for the health and financial industries.
- Instead of storing directly identifiable information such as name or social security number, a health or bank database can store the hash value of this information instead.
- **BLOCKCHAIN, specifically with cryptocurrencies like Bitcoin.**

POPULAR HASHING ALGORITHMS

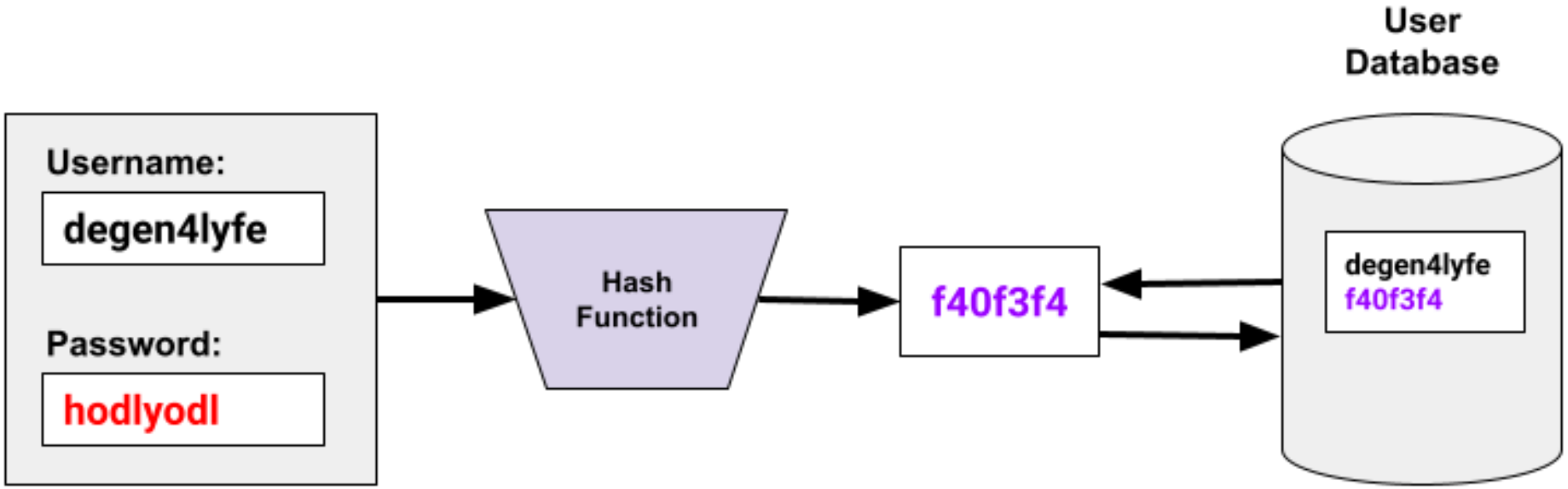
- MD5 (Message Digest5)
- Secure Hash Algorithm (SHA)
- CRC32

How does hashing ensure the integrity of the message?


SENDER
Message
Hashing Algorithm
H1
Message
RECEIVER
If H1 = H2, message is same
RECEIVER
Message
Hashing Algorithm
H2
Message

PASSWORD STORAGE

- Hash functions are commonly used to store passwords securely in databases.
- Instead of storing plaintext passwords, the system stores the hash values of passwords.
- When a user attempts to log in, the system computes the hash value of the entered password and compares it with the stored hash value associated with the user's account.
- If the computed hash value matches the stored hash value, the login attempt is successful.



User signs into email account.

Hash is produced and checked against stored password.

If values are the same, the user is allowed account access.

CRACKING HASHED PASSWORDS

- password
- password1
- password1$
- According to password strength indicator of Cpanel, which one is very weak, weak and strong
- Generate hashes here:
- https://www.md5hashgenerator.com/
- Crack them:
- https://crackstation.net/

DIFFERENCE BETWEEN SYMMETRIC/ ASSYMETRIC AND HASHING CRYPTOGRAPHY?

HOMEWORK

- Read about RSA encryption (Asymmetric)

REFERENCES

- Watkins, S.G.(2008). *An Introduction to Information Security and ISO 27001. A pocket Guide*.UK: IT Governance Publishing
- Andress, J. (2019*). Foundation of Information Security. A straightforward Introduction*. San Francisco: No Starch Press
- Ousley, M. R.(2013). *Information Security*. 2nd edn. Mc Graw Hill Education
- The DES Algorithm Illustrated (tu-berlin.de)
- https://cyberw1ng.medium.com/triple-des-3des-encryption-features-process-advantages-and-applications-2023-587e5a092789