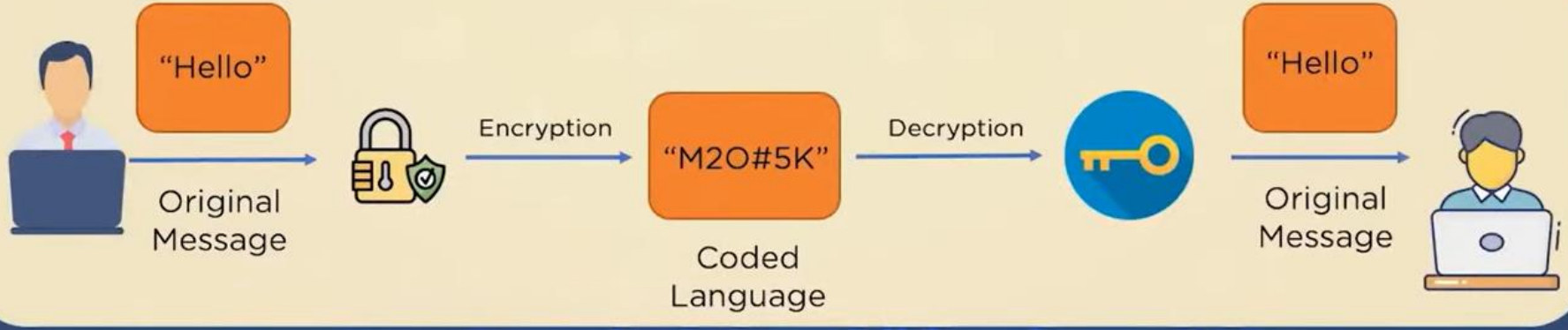
CYBER ENRICH TRAINING PROGRAM | MODULE III

Cryptography

What Is Cryptography?

Cryptography is the science of encrypting and decrypting information to prevent unauthorized access. The decryption process should be known to both the sender and the receiver.



How Does Cryptography Work?

Encryption

Making normal readable text difficult to understand

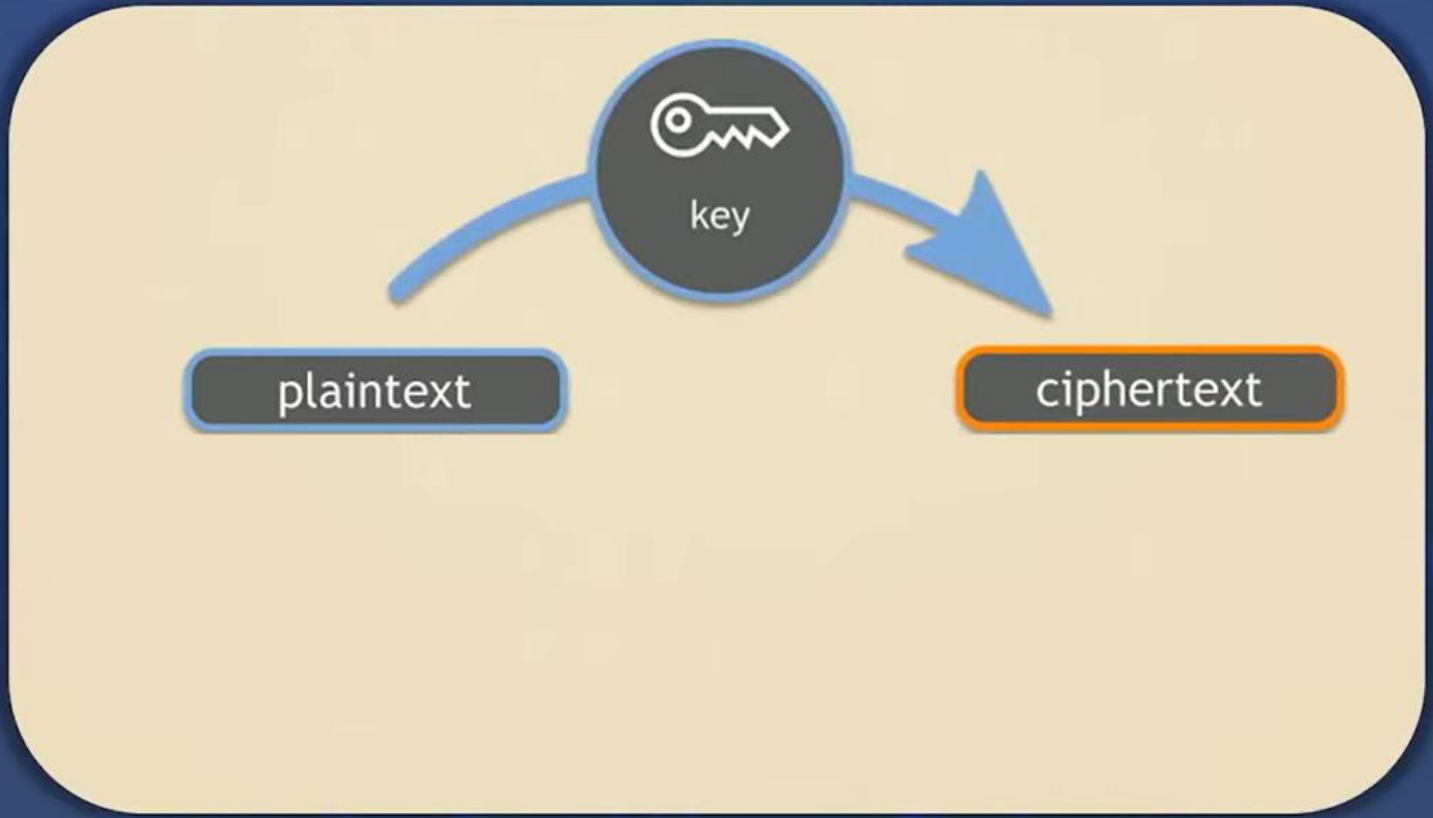
"Hello" → "M2#5K"

Decryption

Reversing the encryption process to retrieve normal message

"M2#5K" → "Hello"

Ciphers and Ciphertext



Transposition Cipher

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext

1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A		T	

Plain Text: MEET ME AFTER PARTY

Key Used: 421635

Cipher Text: TEMEEMEFAPTRYRAT

Substitution Cipher

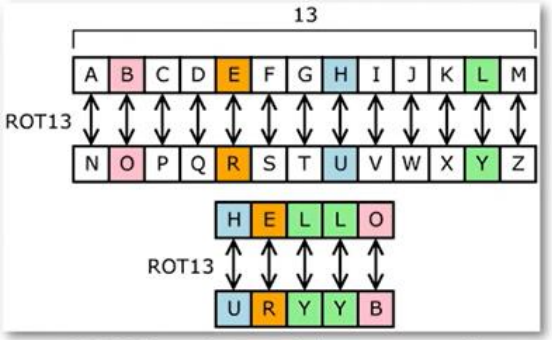
Method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth

Plaintext Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Keyword: Zebras

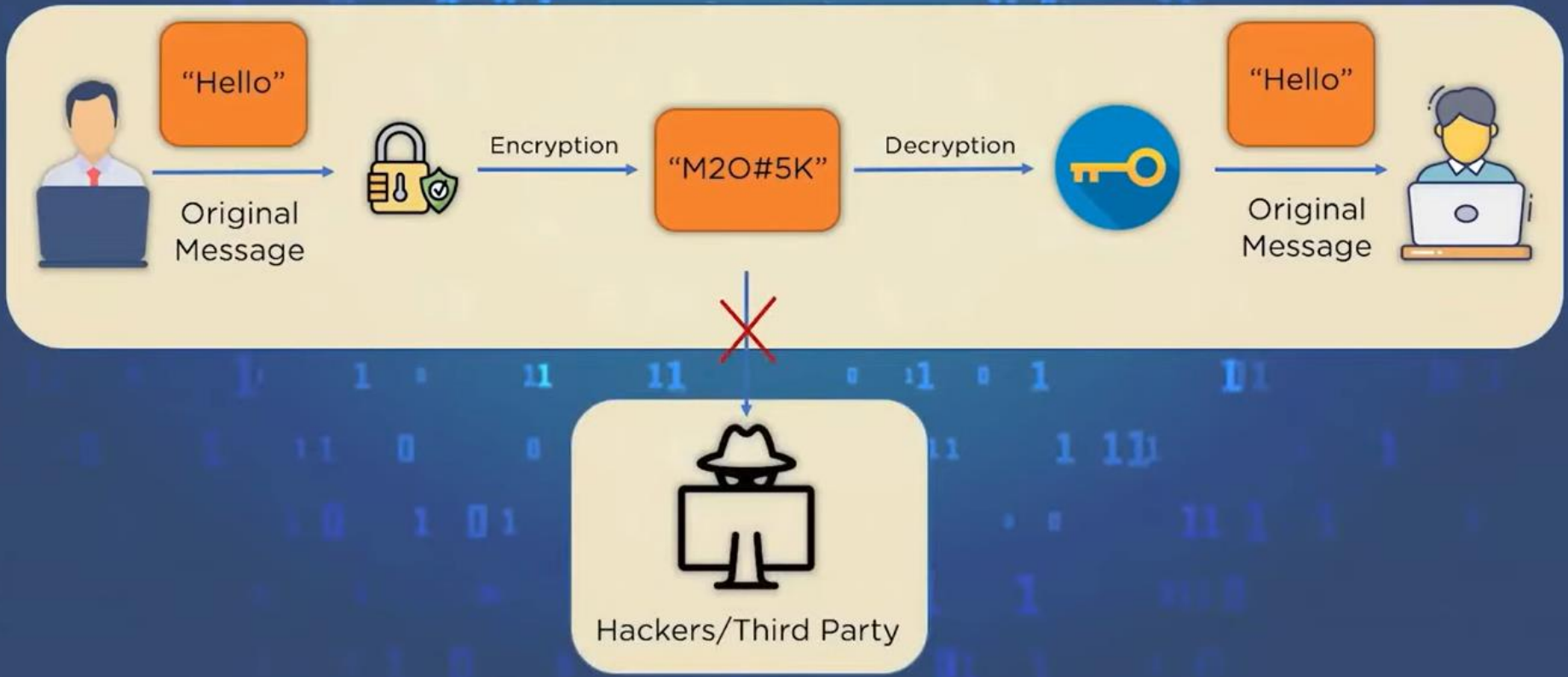
Ciphertext Alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY

A message of: flee at once. We are discovered!
enciphers to: SIAA ZQ LKBA. VA ZOA RFPBLUAOAR!
SIAAZ QLKBA VAZOA RFPBL UAOAR



ROT13 is a Caesar cipher, a type of substitution cipher. In ROT13 alphabet is rotated 13 steps

Ciphers and Ciphertext



Applications of Cryptography

SSL/TLS Encryption

Digital Signatures

Safe Online Banking

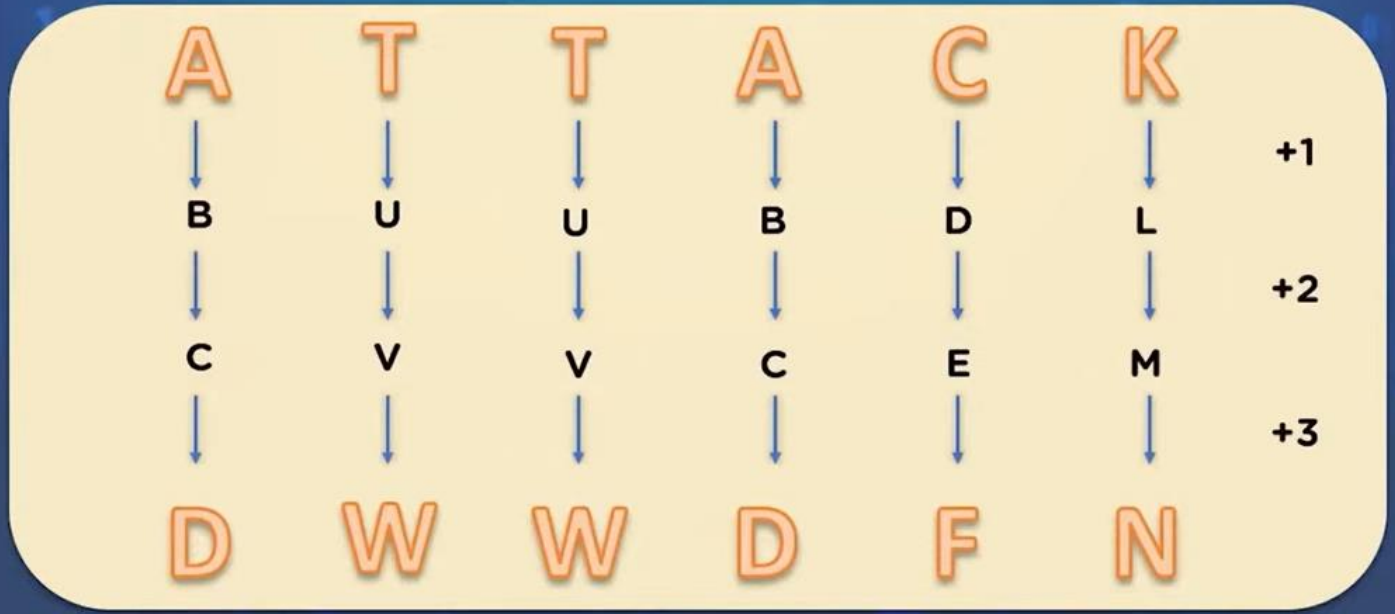
Secure Chatting Services

Encrypted Emails

Crypto-currency

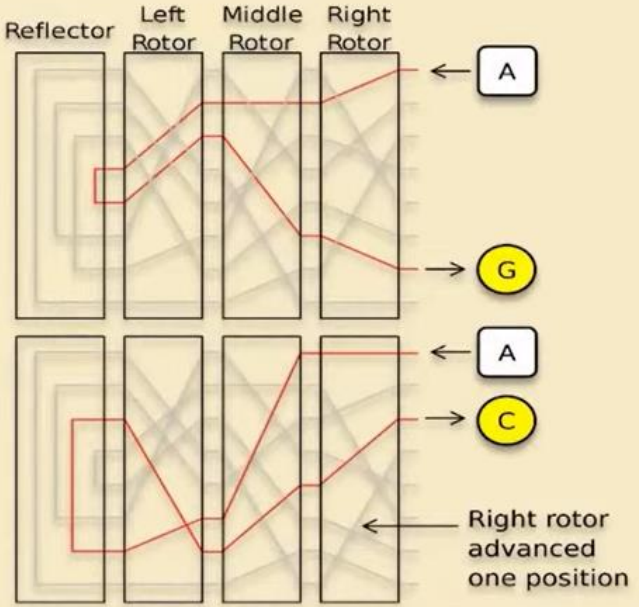
Historical Significance

- Julius Caesar used a substitution cipher, appropriately named Caesar cipher today.
- Alphabets are moved a by a certain number
- If the shift is 1, A becomes B, B becomes C and so on.

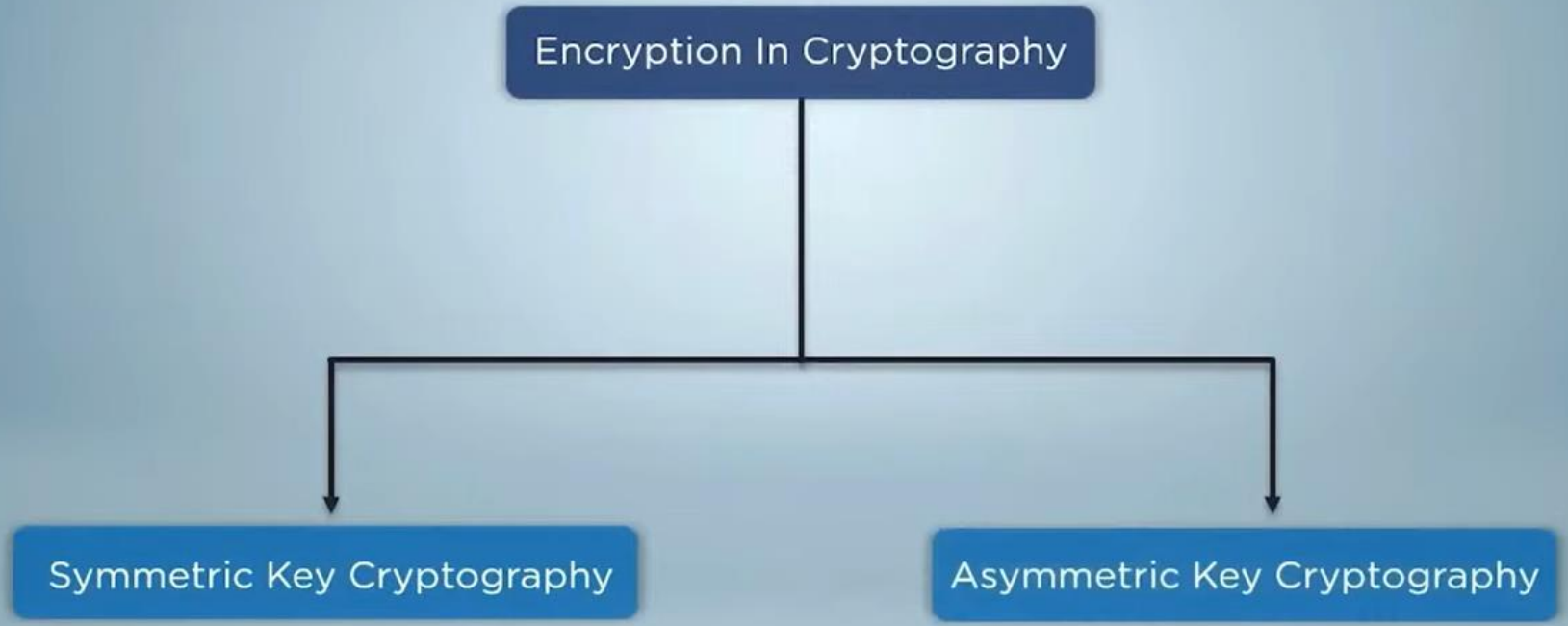


The Enigma Machine

- Developed and used by Nazi German armies in the World Wars
- Used to protect confidential information during transit
- Electromechanical signals generate random alphabets



Types of Encryption



Applications of Symmetric Key Cryptography

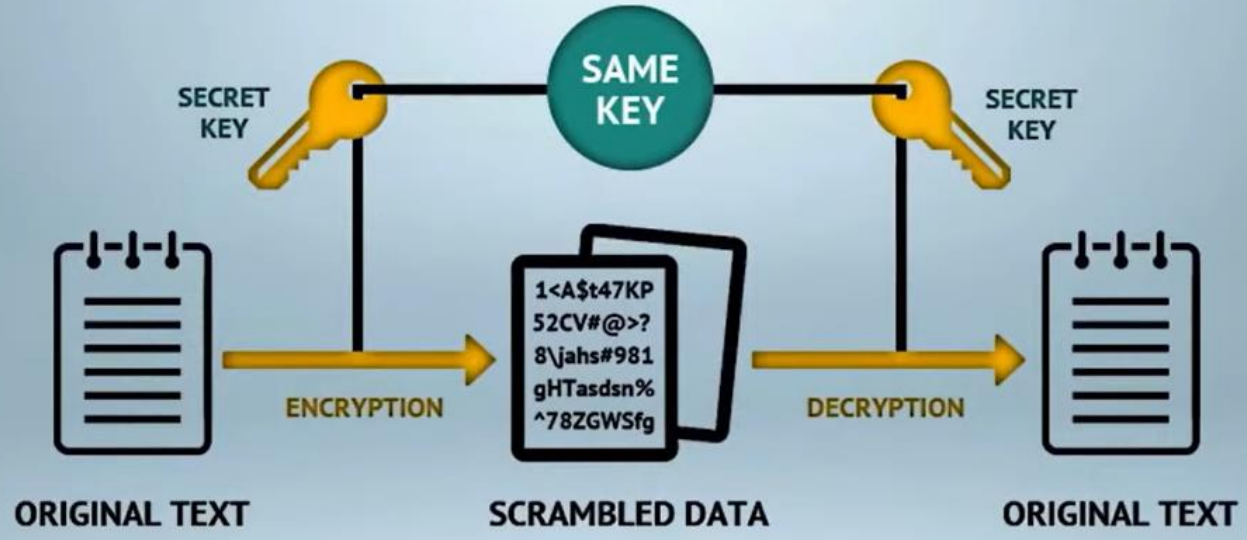
Banking applications to authenticate ID and transactions

Server/Data Center information can be encrypted at rest

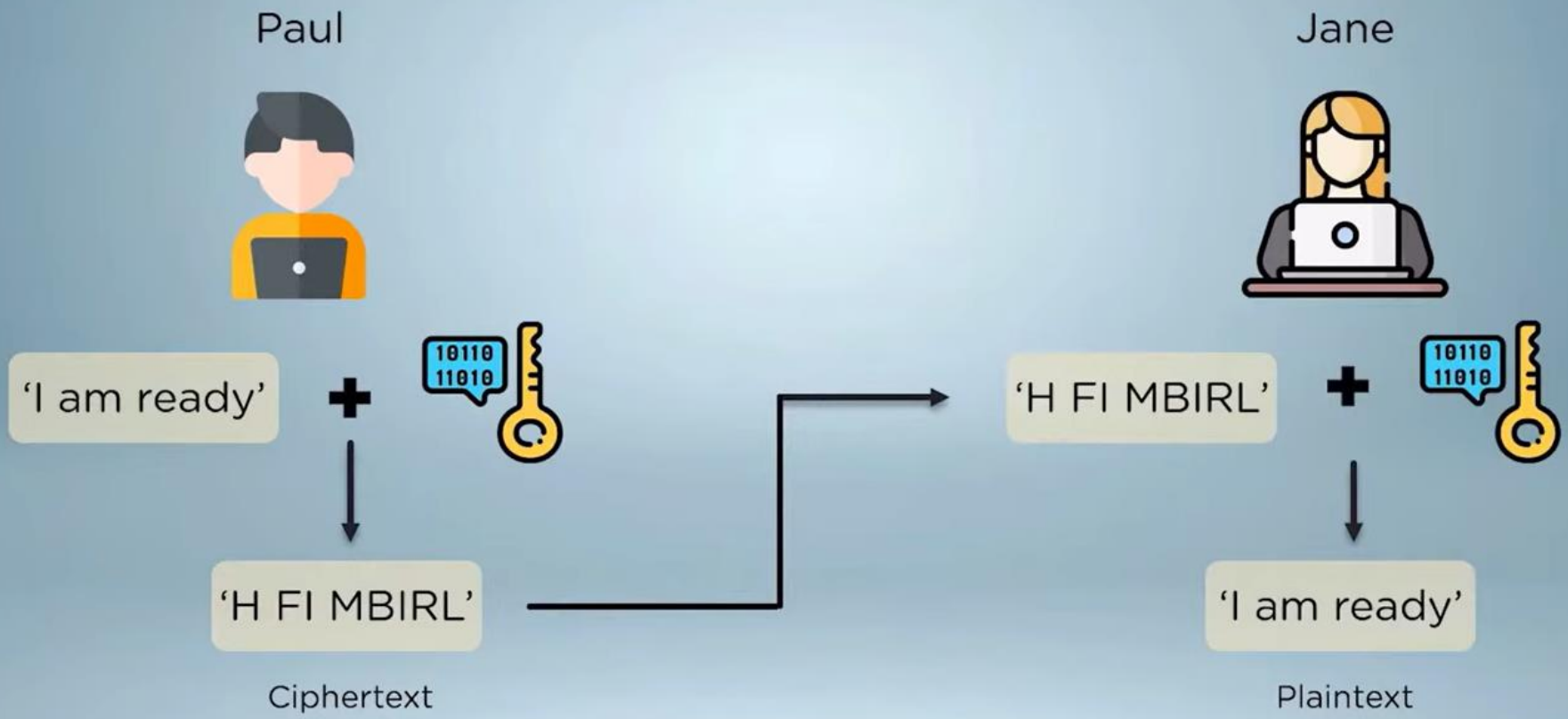
HTTPS encryption with secure all-around browsing

What Is Symmetric Key Cryptography?

Symmetric Key Cryptography relies on a single key for encryption and decryption of information. The key needs to be kept secret and be available with both the sender and receiver. Strength of encryption depends on the key size being used.



What Is Symmetric Key Cryptography?



Private – Key Cryptography

- Same Key for encryption and decryption means a single point of failure
- Key needs to be always kept secret
- Receiver/Third party can also generate messages with the same key, so authentication issue will arise should the secret key is leaked

Types of Encryption – Stream Ciphers

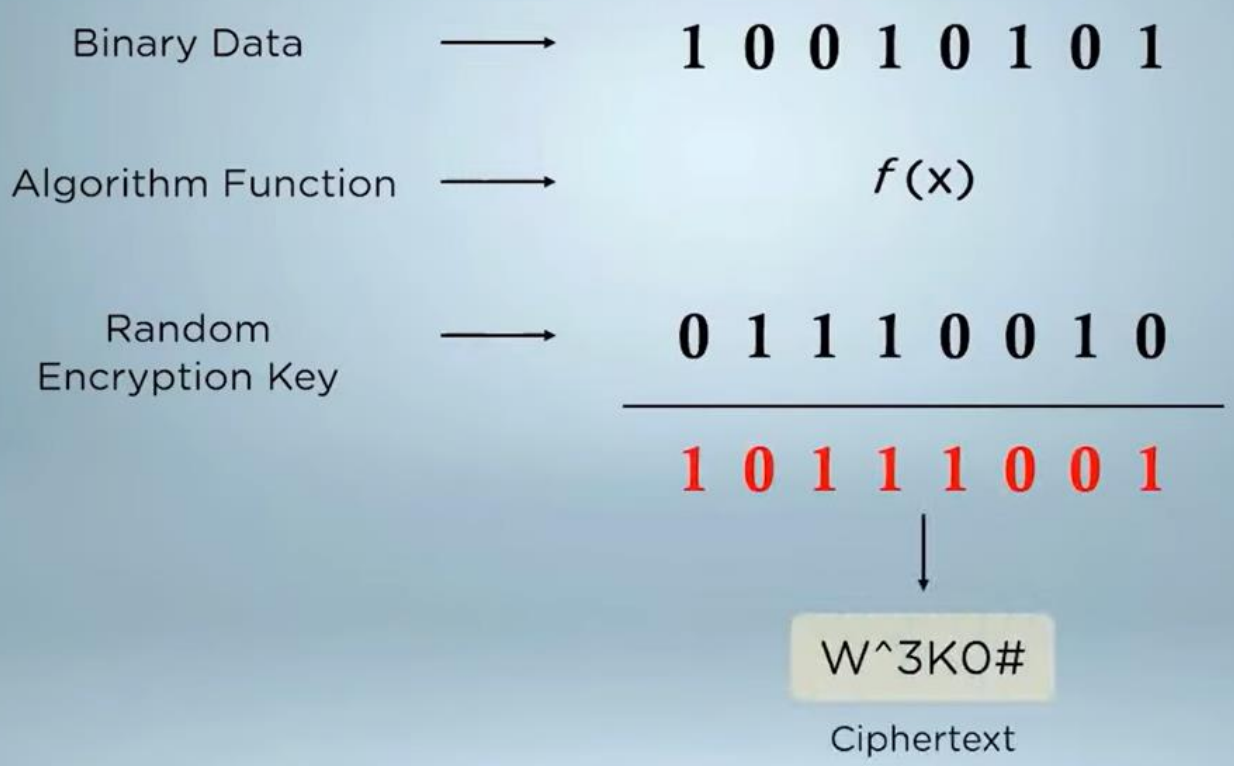
- Encrypt information one bit/byte at time
- Quicker format of encryption
- Data is converted to binary digits and encrypted sequentially
- Popular algorithms – RC4, Salsa20

Binary Data

Encryption Key

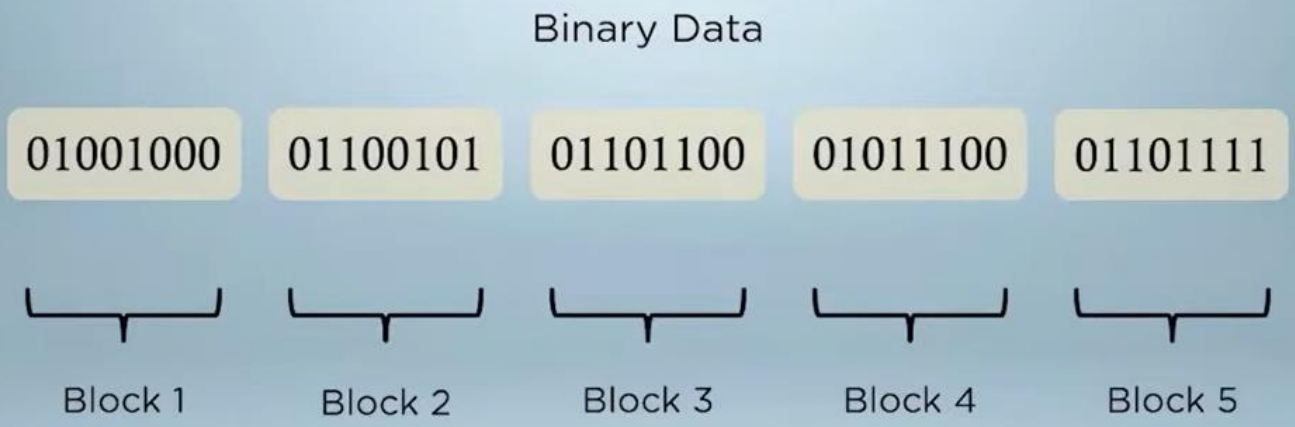
Ciphertext

Types of Encryption – Stream Ciphers

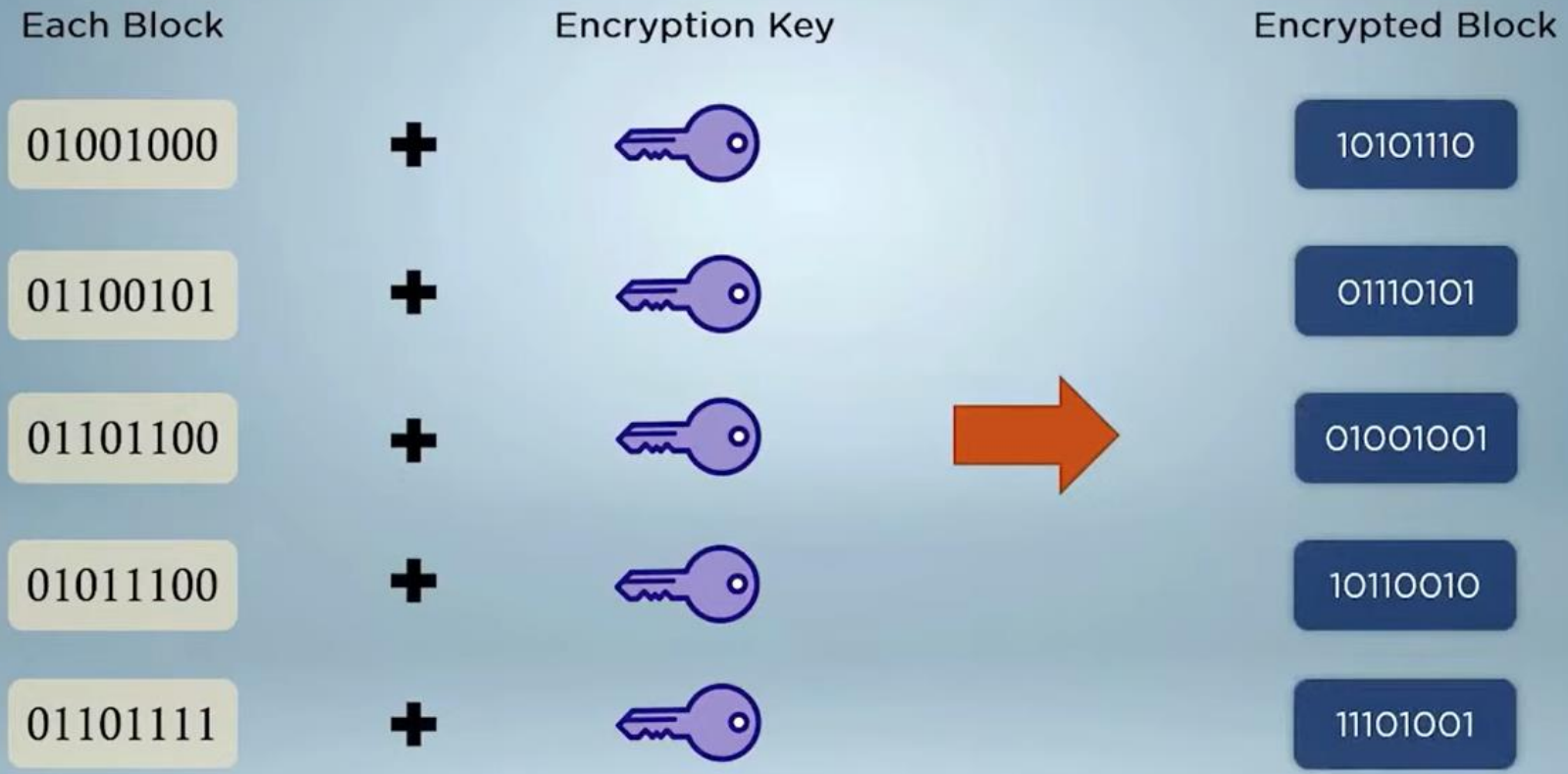


Types of Encryption – Block Ciphers

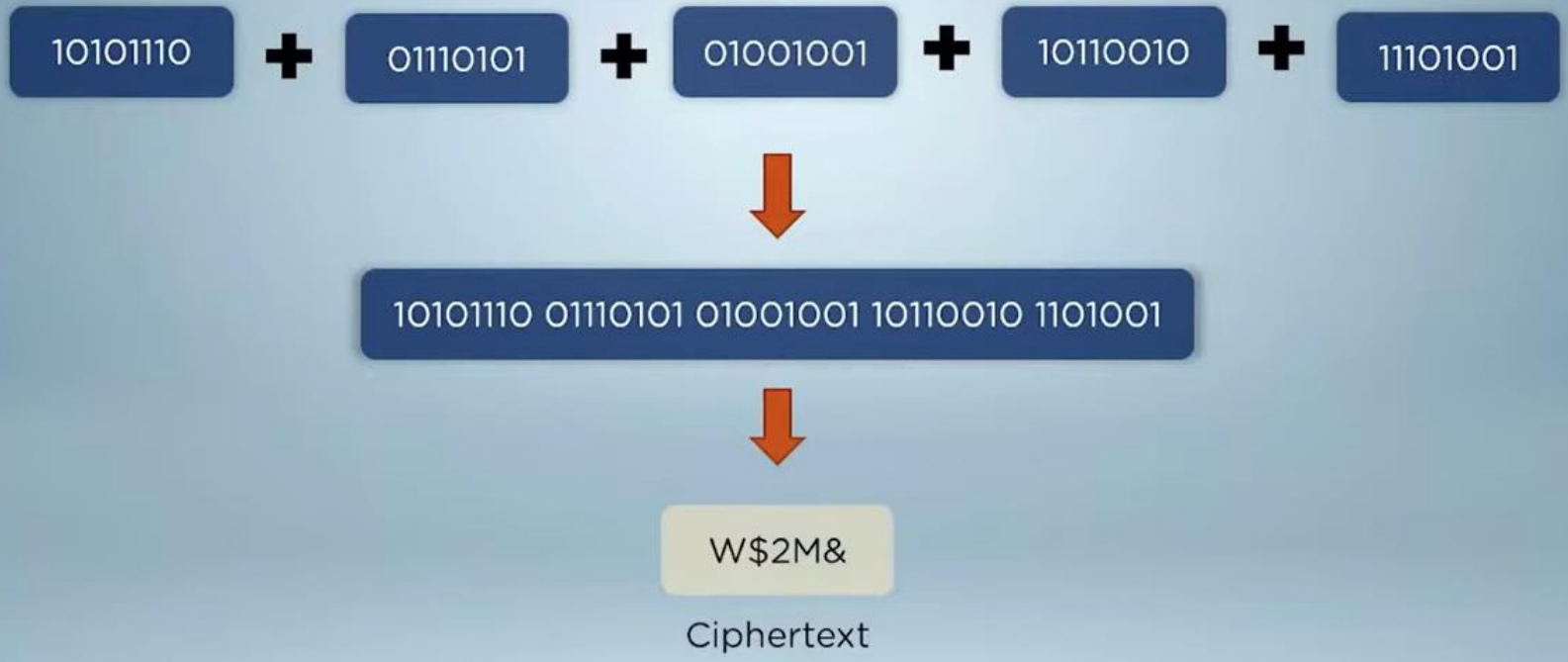
- Information broken down to chunks/blocks of fixed size
- Size of block depends on key size
- The chunks are encrypted and later chained together
- Popular algorithms – AES, DES, 3DES



Types of Encryption – Block Ciphers



Types of Encryption – Block Ciphers



Advantages of Symmetric Key Cryptography

Faster than Asymmetric

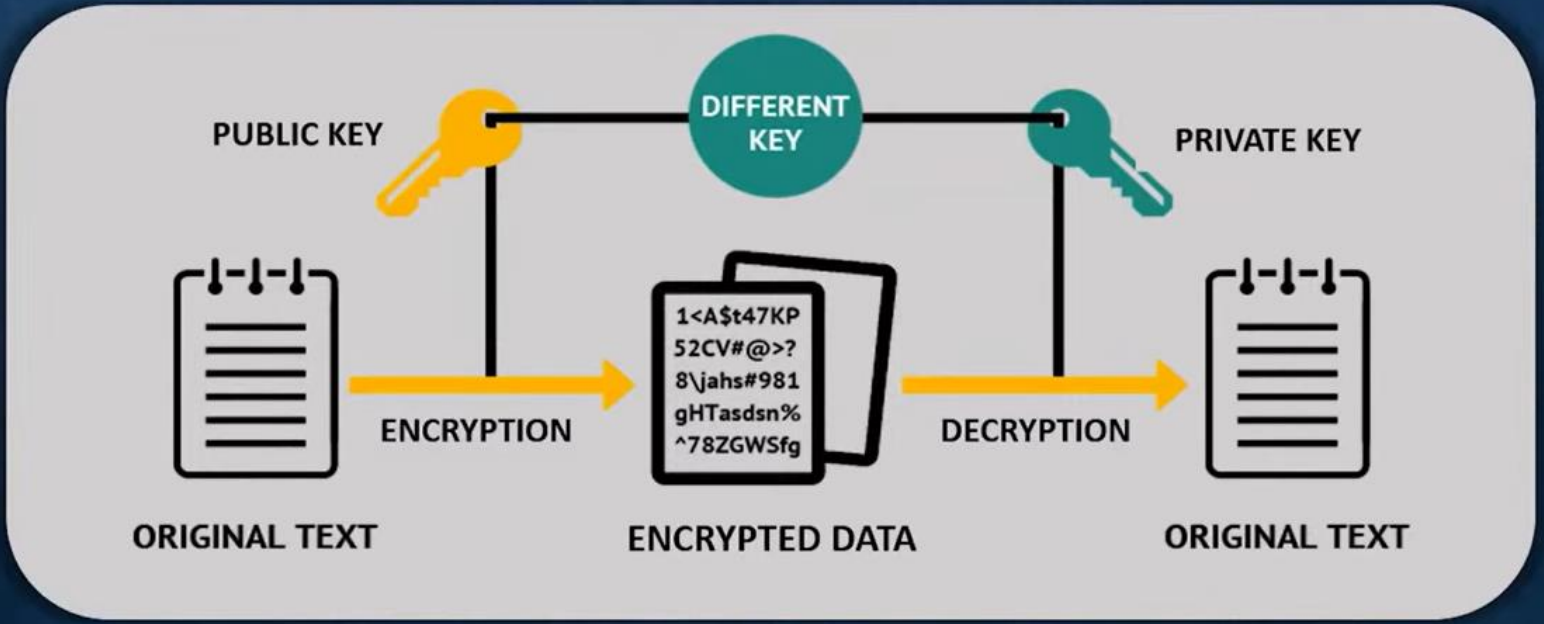
Better Performance Metrics

Optimized for bulk amounts of data

Easier to set-up and implement

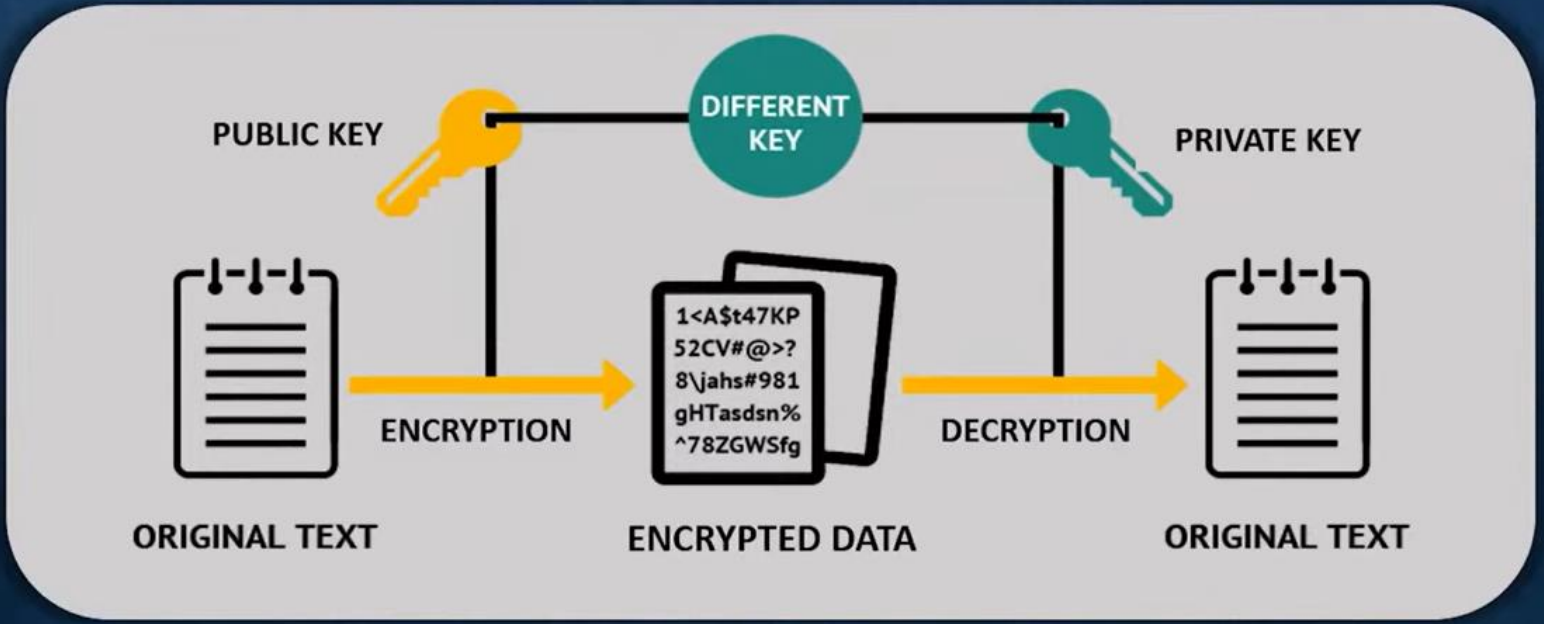
What Is Asymmetric Key Cryptography?

Asymmetric Key Cryptography uses **two different keys** for encryption and decryption. The key used for **encryption** is the **public key**, and the key used for **decryption** is the **private key**.



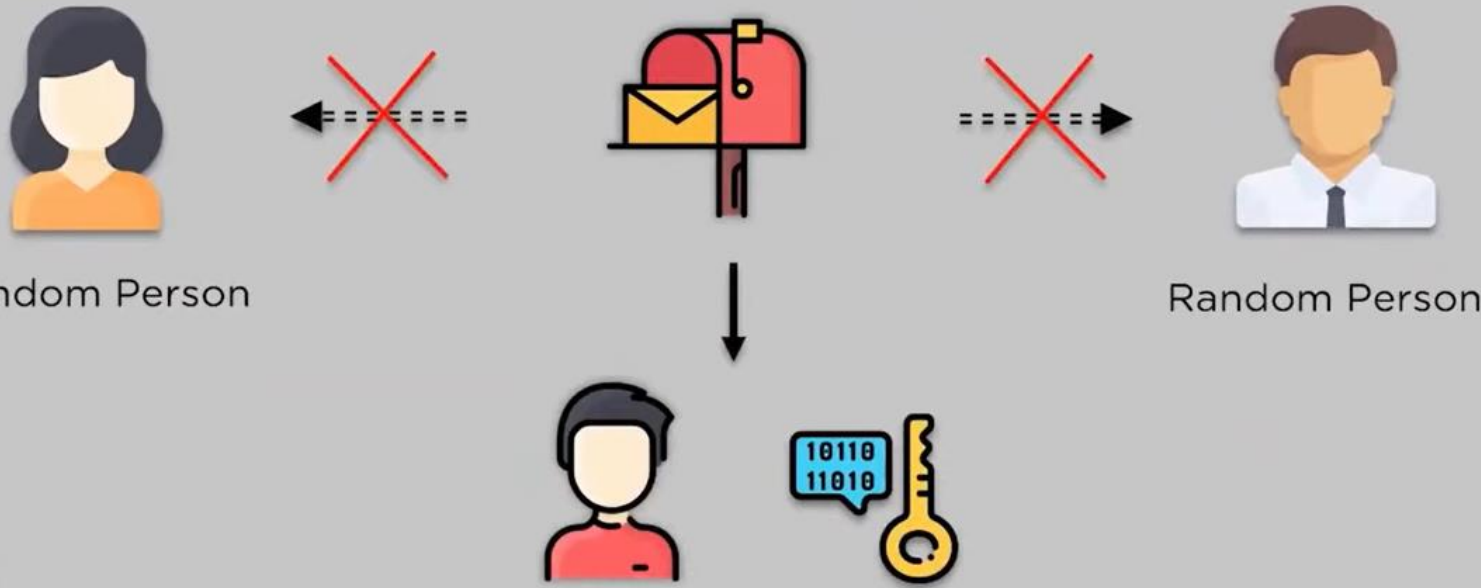
What Is Asymmetric Key Cryptography?

Asymmetric Key Cryptography uses **two different keys** for encryption and decryption. The key used for **encryption** is the **public key**, and the key used for **decryption** is the **private key**.

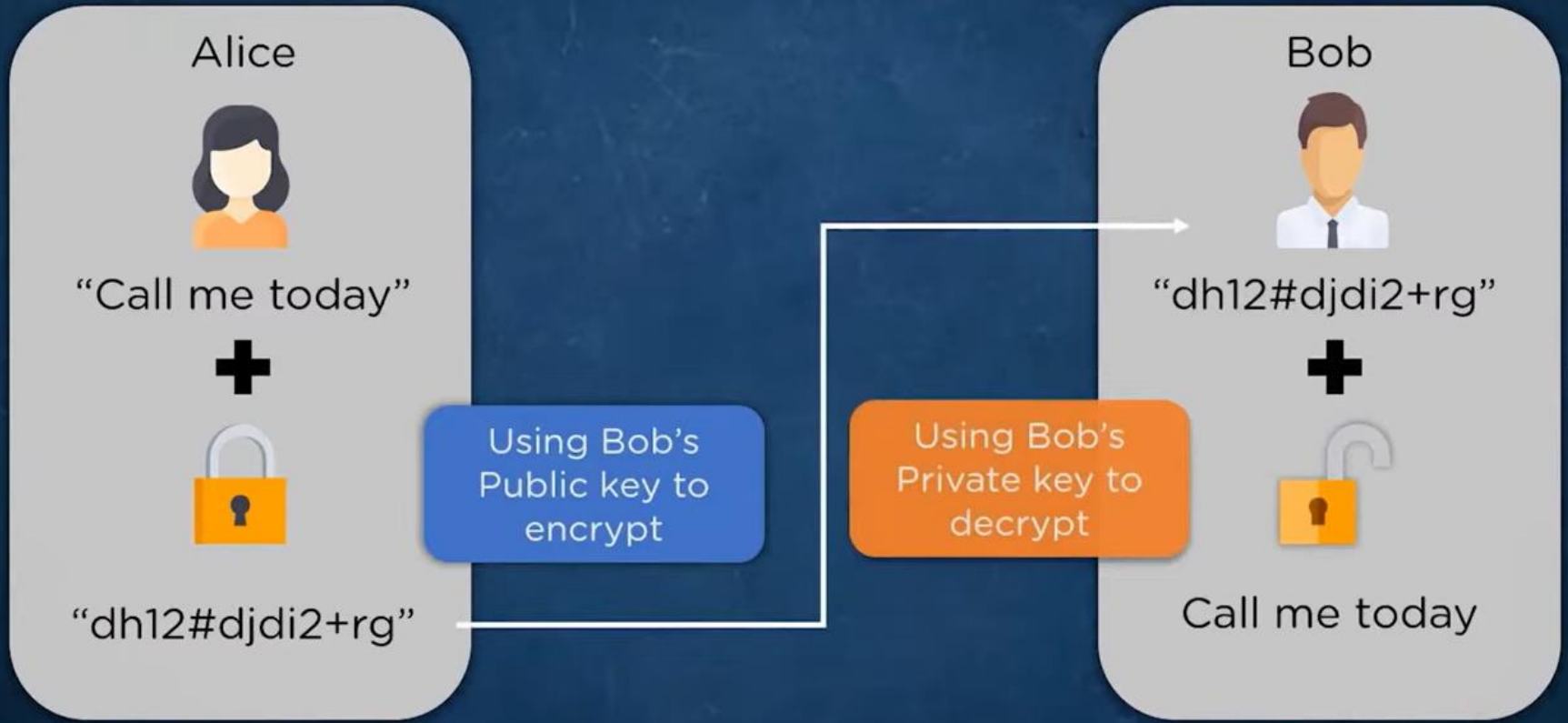


What Is Asymmetric Key Cryptography?

However, nobody other than you can access the contents of the mailbox since only you have the key that can unlock it.



What Is Asymmetric Key Cryptography?



Applications of Asymmetric Key Cryptography

Digital Signatures to maintain authenticity of documents

Encrypted browsing sessions for better protection against hackers

Managing **Crypto-currency transactions** securely

Sharing Keys for Symmetric Key Cryptography

Why Asymmetric Cryptography Is Called Public Key Cryptography?

Encryption Key

Publicly Available

Decryption Key

Privately Stored

Advantages Over Symmetric Cryptography

No need of sharing secret keys

Proof of owner's authenticity

Longer Key lengths mean stronger encryption

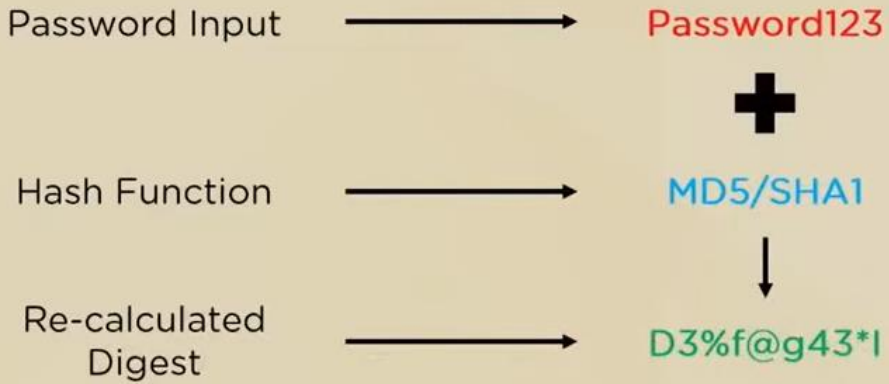
Data can't be modified in transit

What Is Hashing?

Hashing is the process of scrambling a piece of information or data beyond recognition. They are designed to be **irreversible**. We pass the input through a hash function to calculate the **Hash Value** or **Digest**.

Real-World Implementation

When the same user tries to log-in, the password they input is passed through the function again and the digest is compared to the one stored on the servers.



Real-World Implementation

If the re-calculated hash matches the hash stored on the servers during initial sign-up, the log-in is allowed.

D3%f@g43*l

Re-calculated Digest

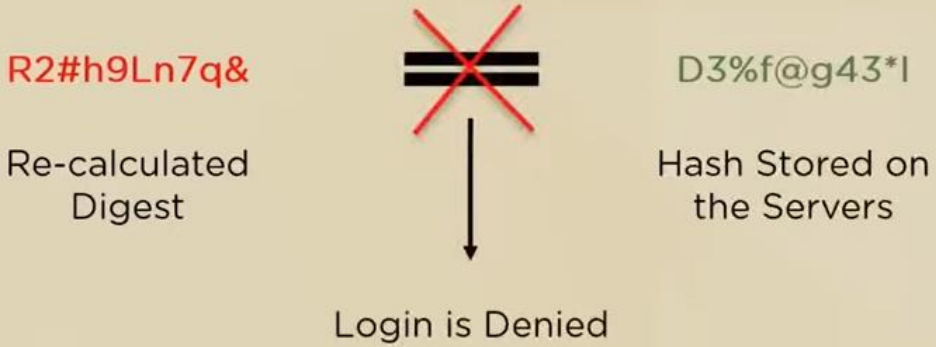
D3%f@g43*l

Hash Stored on the Servers

Login is Allowed

Real-World Implementation

If the calculated digest is different from the one on the server, the login is denied from the website.



Hash Functions

- **Mathematical operations** to be carried out on two blocks of data.
- Both blocks are created by **dividing** the initial input into equal parts.
- **Irreversible** by design.
- Can be carried out multiple times, but the **final digest** must be consistent for the same input.

Hash Algorithm	Digest Size
MD5	128 bits
SHA-256	256 bits

Hashing Guidelines

Hash function must be fast, but not instantaneous

- Should be able to hash in-mass with a reasonable limit to **prevent exploitation.**
- Ultra quick algorithms can be tested rigorously for **brute force** attacks.
- With enough brute force attacks, not just the hash, enti

Hashing Guidelines

Hash digest must be dependent on each bit

- If a single character changes, a **substantial portion** of the digest must change.
- Helpful in creating as many **unique hashes** as possible.
- Hash digest for the plaintext 'Cryptography' will be **completely different** than when the plaintext is 'Cryptograph'.

Hashing Guidelines

Prevent Hash Collision

- Collision occurs when there are two exactly **same hash values/digests.**
- Since there is only one hash function for each server, **same passwords** have **same digests** after hashing.
- **Salting** can help prevent collisions, as we will learn later in this lesson.

Salting

- Salting is the process of **adding a random keyword** to the end of the input.
- The random keyword added is called the **salt/salt value**.
- The salt is **unique** for each user in the database and is helpful to battle hash collision.

Input into Hash Function	MD5 Hash Value/Digest
Cryptography	d2fc0657a64a3291826136c7712abbe7
Cryptographyabc123	c56db83ab5482b4e94536f4a29b21de0
Cryptographyxyz456	783b10b483435e05f3f2705bdd5a825c

Peppering

- Peppering is the process of adding the **same random value** at the end of a plaintext.
- Since it doesn't change per user, the random value **need not be stored** on server.
- In the case of a data breach, pepper value is **safe from further exploitation**.

Input into Hash Function	MD5 Hash Value/Digest
CryptographyRan123	4cac3f25fffad414e834ee8208f65116
MyPasswordRan123	470dd61e2acce64486e784f3a288d82f
Qwerty101Ran123	a8792a61ee831c39548ec1a2e1ba3d68

Key Generation

1. Two large prime numbers are chosen (**p** and **q**)

2. Compute $n = p * q$ and $z = (p-1)(q-1)$

3. Choose a number **e** where $1 < e < (p-1)(q-1)$

4. A number **d** is selected so that **ed mod** $z = 1$ and calculated as $d = e^{-1} \bmod (p-1)(q-1)$

5. Public key is **(n,e)** and private key is **(n,d)**

Encryption and Decryption

If the plaintext is **m**, encrypted ciphertext **c** is calculated as:

$$c = m^e \bmod n$$

Under similar assumptions, the plaintext can be calculated as:

$$m = c^d \bmod n$$

Data Encryption- Example

1. Choose p and q as 7 and 13 respectively, so that $n=p*q=91$
2. We can select value of **e** to be **5** since it satisfies $1<e<(p-1)(q-1)$
3. Value of **d** = $e^{-1} \bmod (p-1)(q-1) = 29$
4. Public key = (91,5), private key = (91,29)
5. Let plaintext **m** be **10**.

   Ciphertext(c) = $m^e \bmod n = 82$
   Plaintext = $c^d \bmod n = 10$