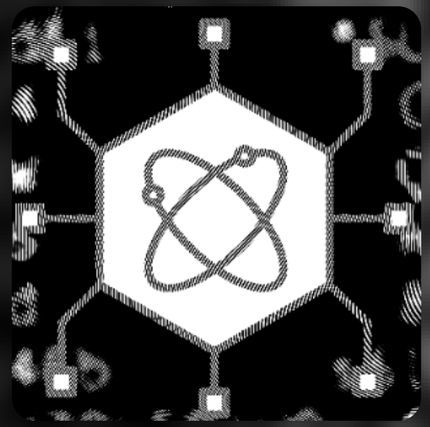
1337

THE ELITES' SECURITY



CYBER SECURITY & CRYPTOGRAPHY

INTRODUCTION TO CRYPTOGHRAPHY

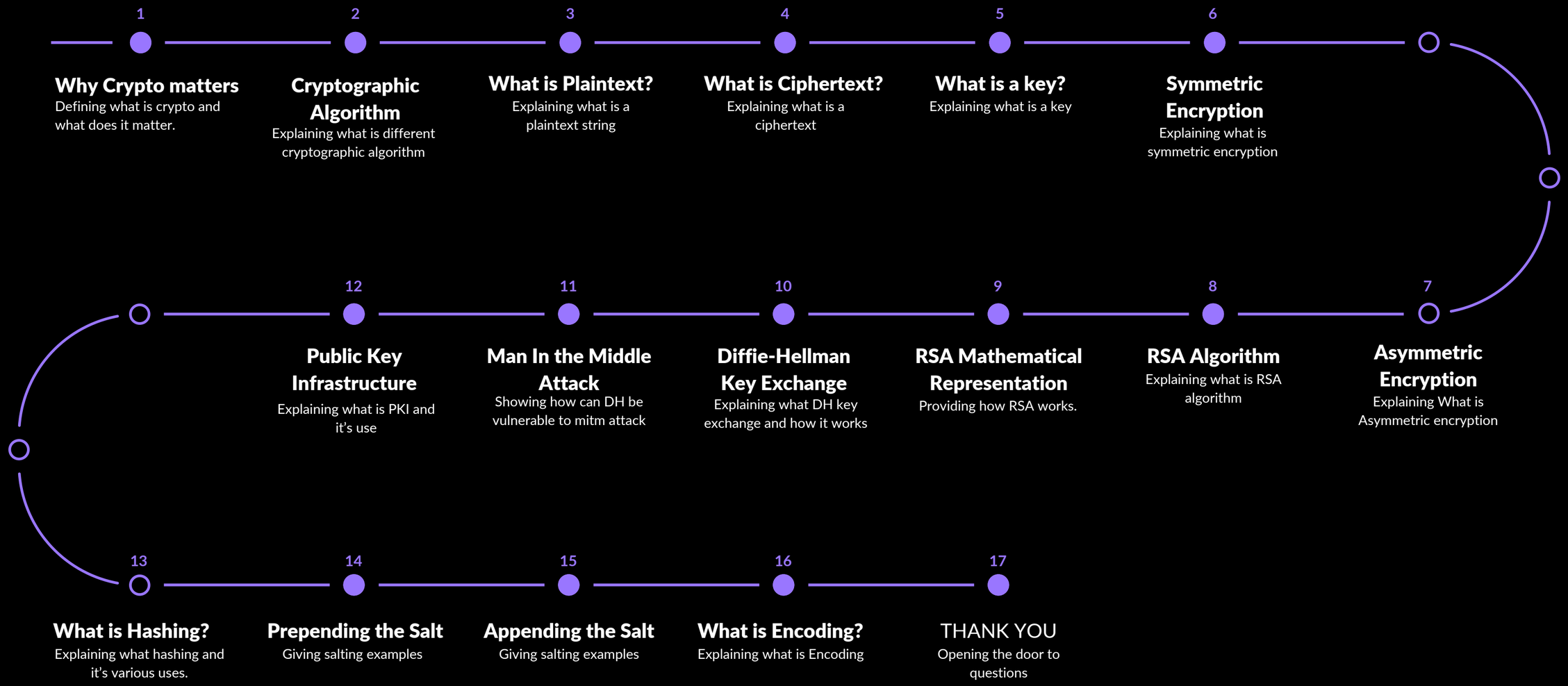
An overview of the most common cryptographic methods and algorithms.

Ashad Mohamed
Security Researcher

1337

THE ELITES' SECURITY

TABLE OF CONTENT



1337

THE ELITES' SECURITY

Why Cryptoghraphy Matters

Cryptography is one of the most **important** tools **businesses** use to **secure** the **systems** that hold its most important **asset** whether it is at-rest or in-motion.

Cryptographic Algorithm

A **cryptographic** algorithm is the **mathematical** equation used to scramble the **plain text** and make it **unreadable**.

What is Plaintext?

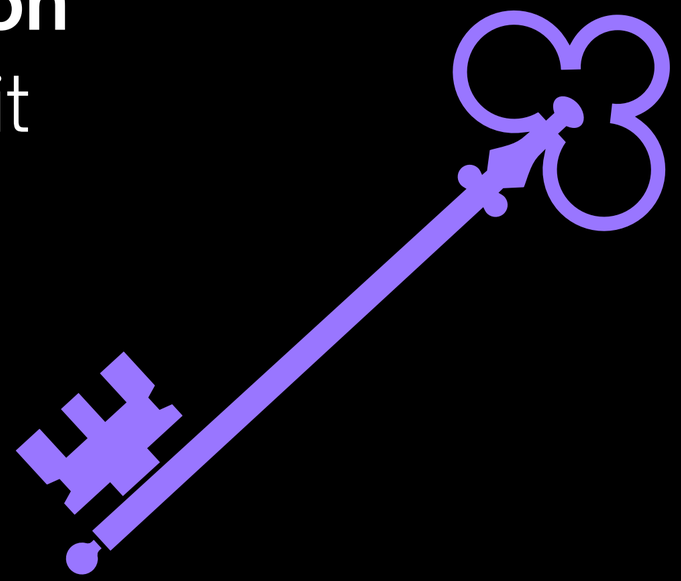
Readable and **understandable** data that is given to an **encryption algorithm** as an **input.**

What is Ciphertext?

Output of **encryption algorithm** in an **unintelligible** form that one **cannot** understand.

What is a key?

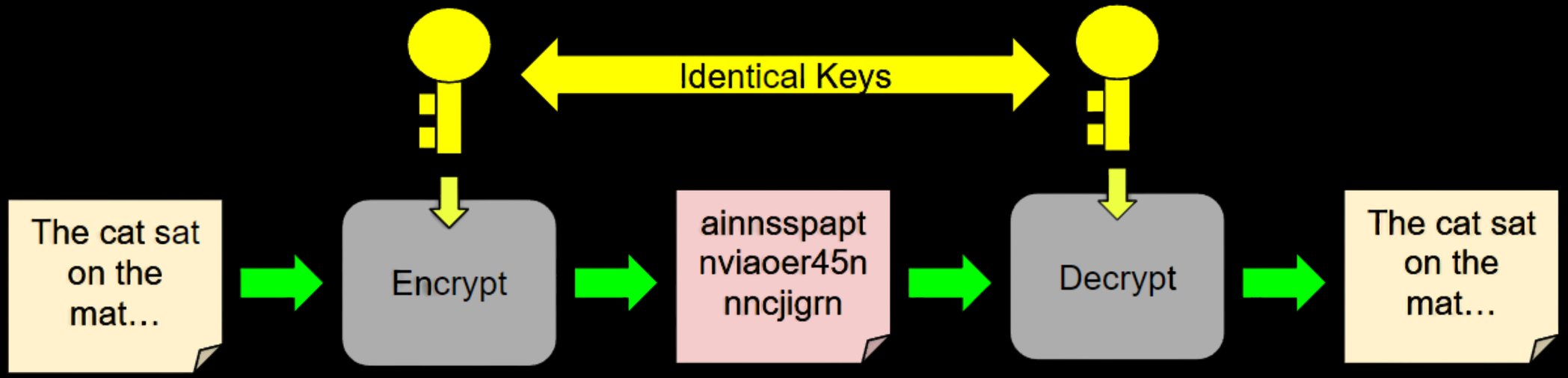
In **cryptography**, a **key** is a string of characters used within an **encryption algorithm** for **altering** data so that it **appears random**.



Symmetric Encryption

Symmetric Encryption is an **Algorithms** that use the same **cryptographic keys** for both the **encryption** of **plaintext** and the **decryption** of **ciphertext**.

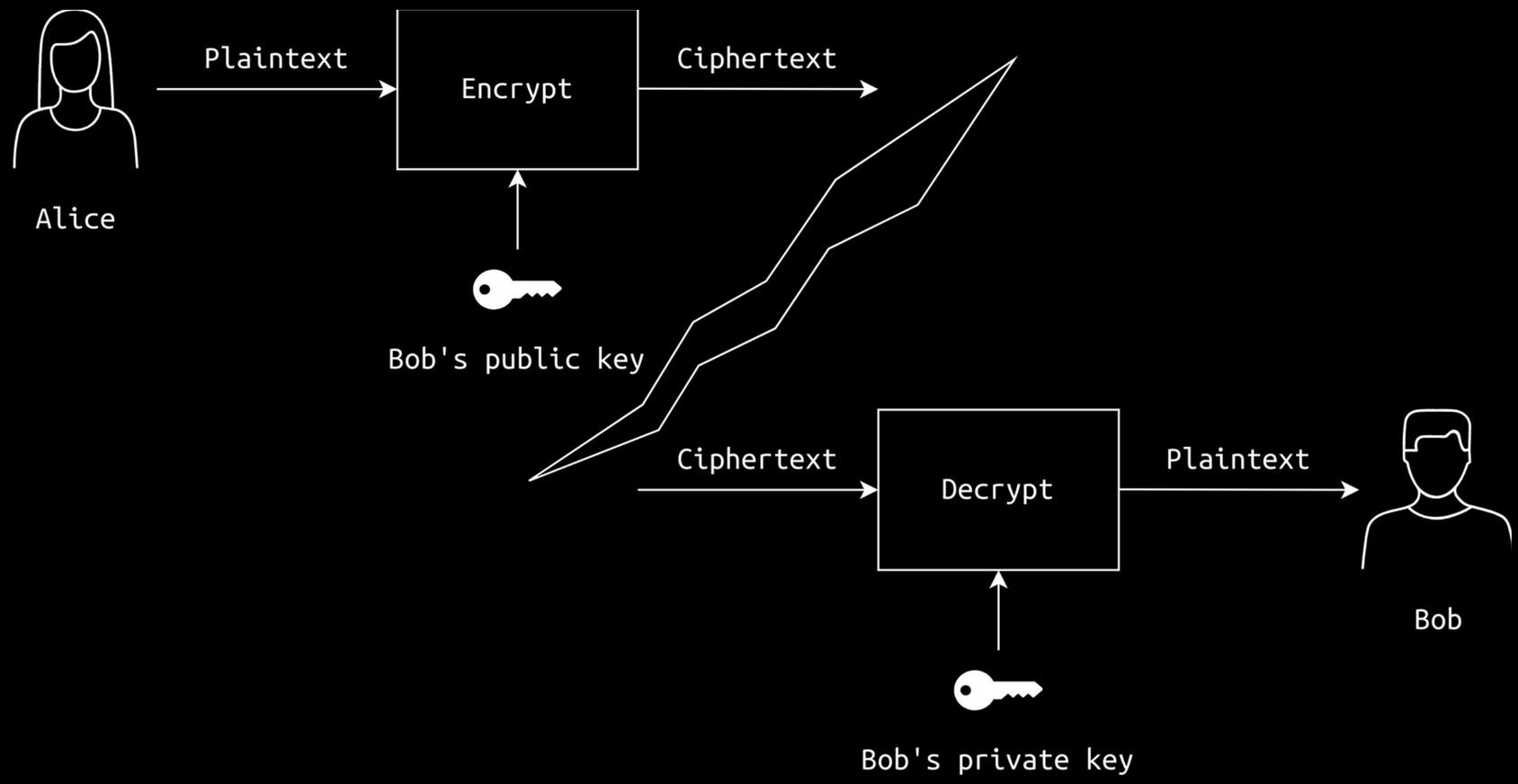
Symmetric Encryption



Asymmetric Encryption

Asymmetric Encryption or **Public-key cryptography**, uses **two different keys** - a **private key** and a **public key**. The private key is **kept secret**, while the public key is **shared freely**.

Asymmetric Encryption



RSA Algorithm

RSA is a **public-key** cryptosystem, one of the **oldest**, that is **widely** used for secure **data transmission**.

1337

THE ELITES' SECURITY

RSA Mathematical Representation

1. Choose two random prime numbers, **p** and **q**. Calculate ***N = p × q***.

2. Choose two integers **e** and **d** such that **e × d = 1 mod ϕ(N)**, where: $\phi(N) = N - p - q - 1$

This step will let us generate the public key **(N,e)** and the private key **(N,d)**.

3. The sender can encrypt **a** value **x** by calculating: $y = x^e mod N$

4. The recipient can decrypt y by calculating: $x = y^d mod N$

Diffie-Hellman Key Exchange

Diffie-Hellman (DH) is a cryptographic **protocol** that **enables** two parties to agree on a **shared secret key** without prior **knowledge** of each other.

Diffie-Hellman Key Exchange

Alice

Chooses a

Sends A

0 Agree on q and g; e.g., 29 and 3

1 $A = g^a \bmod q = 3^{13} \bmod 29 = 19$

$B = g^b \bmod q = 3^{15} \bmod 29 = 26$ 2

Chooses b

Sends B

Bob

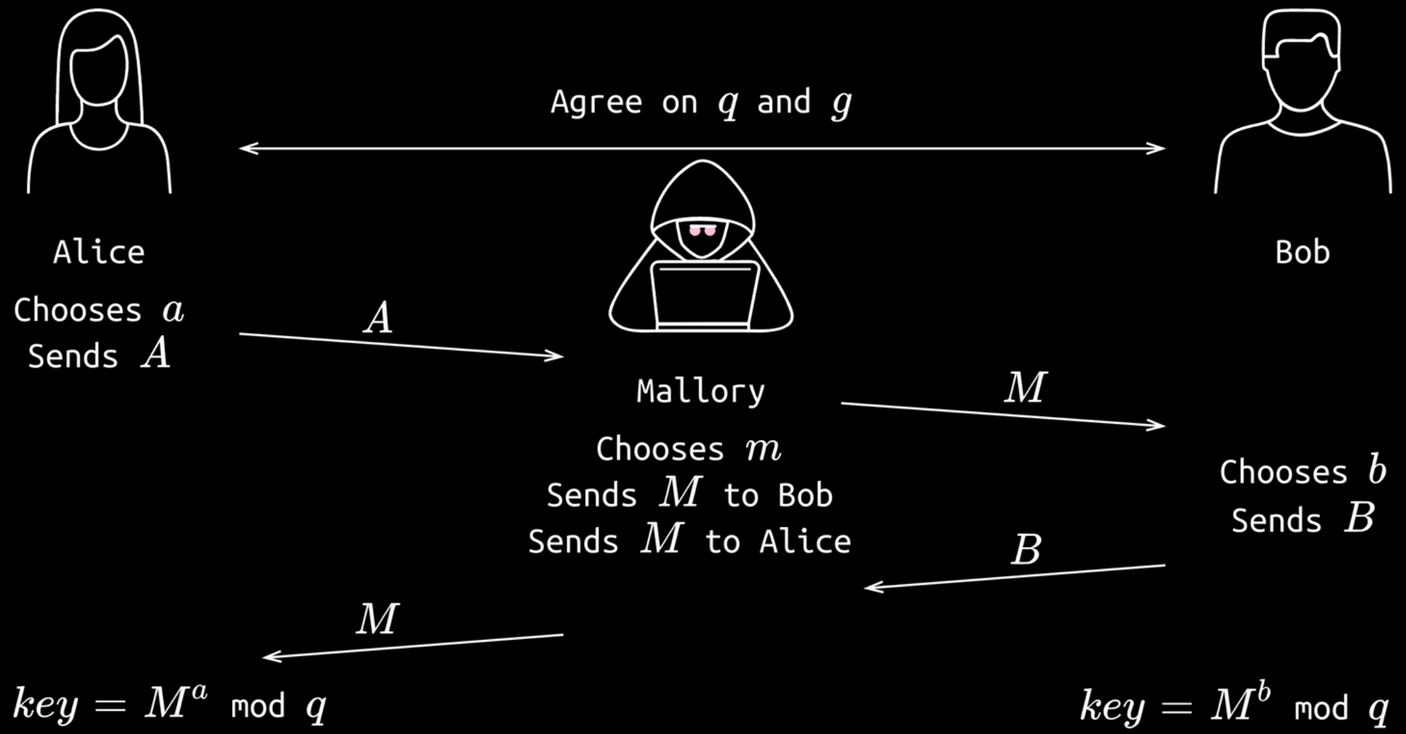
3 $key = B^a \bmod q$

$= 26^{13} \bmod 29 = 10$

4 $key = A^b \bmod q$

$= 19^{15} \bmod 29 = 10$

Man In the Middle Attack



The Diffie-Hellman (DH) key exchange is **vulnerable** to a **man-in-the-middle** attack.

1337

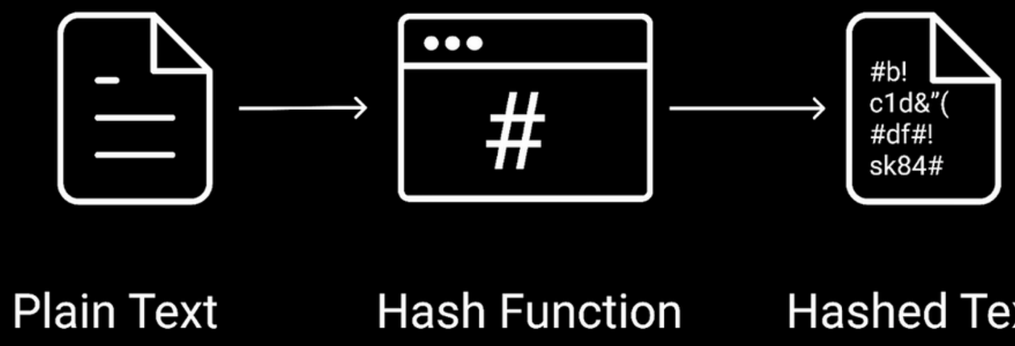
THE ELITES' SECURITY

Public Key Infrastructure

Public Key Infrastructure (PKI) is a set of **rules** and **policies** that makes it possible for **different entities** to communicate **securely** over a **network**.

What is Hashing?

A **hash function** is a **mathematical algorithm** that takes an **input** (or ‘message’) and returns a **fixed-size string** of bytes, usually in the form of a **hexadecimal number.**



Message Digest Method 5

MD5 a cryptographic **hash algorithm** used to generate a **128-bit** digest from a **string of any length.**

Salting

Adding random **data** to the **input of a hash** function to **guarantee** a unique output, the **hash**, even when the **inputs are the same**.

Prepending the Salt

Password: hello@/0-2freesh
Salt: datae8300kd/as
Salted Input: datae8300kd/ashello@/0-2freesh

Hash (SHA-256):
f5ac26a91c388aaff9bd849a03ce888b91f1cf7474b07d68ea554d78d7426740

```
e2r1p8% echo -n  "datae8300kd/ashello@/0-2freesh" | openssl sha256
SHA2-256(stdin)= f5ac26a91c388aaff9bd849a03ce888b91f1cf7474b07d68ea554d78d7426740
```

Appending the Salt

Password: hello@/0-2freesh
Salt: datae8300kd/as
Salted Input: hello@/0-2freeshdatae8300kd/as

Hash (SHA-256):
614690e6eaf823b189bae26fc046e13598d67effeee253f4231305ae1832f1e3

```
e2r1p8% echo -n  "hello@/0-2freeshdatae8300kd/as" | openssl sha256
SHA2-256(stdin)= 614690e6eaf823b189bae26fc046e13598d67effeee253f4231305ae1832f1e3
```

What is Encoding?

Encoding is the process of transforming a set of Unicode characters into a **sequence of bytes**.

THANK YOU FOR YOUR ATTENTION

Any questions?