What is Asymmetric Encryption?

Understand with Simple Examples

Learn what Asymmetric Encryption is, how it works, and what it does

Table of Content

- How does Asymmetric Encryption work?
- How are the two keys generated?
- Difference between Symmetric and Asymmetric Encryption

All about
Asymmetric Encryption

“

Asymmetric Encryption, also known as Public-Key Cryptography

- When it comes to the word ‘**Encryption**,’ we think of it as a technique that protects data using a cryptographic key, and there’s nothing wrong with this.

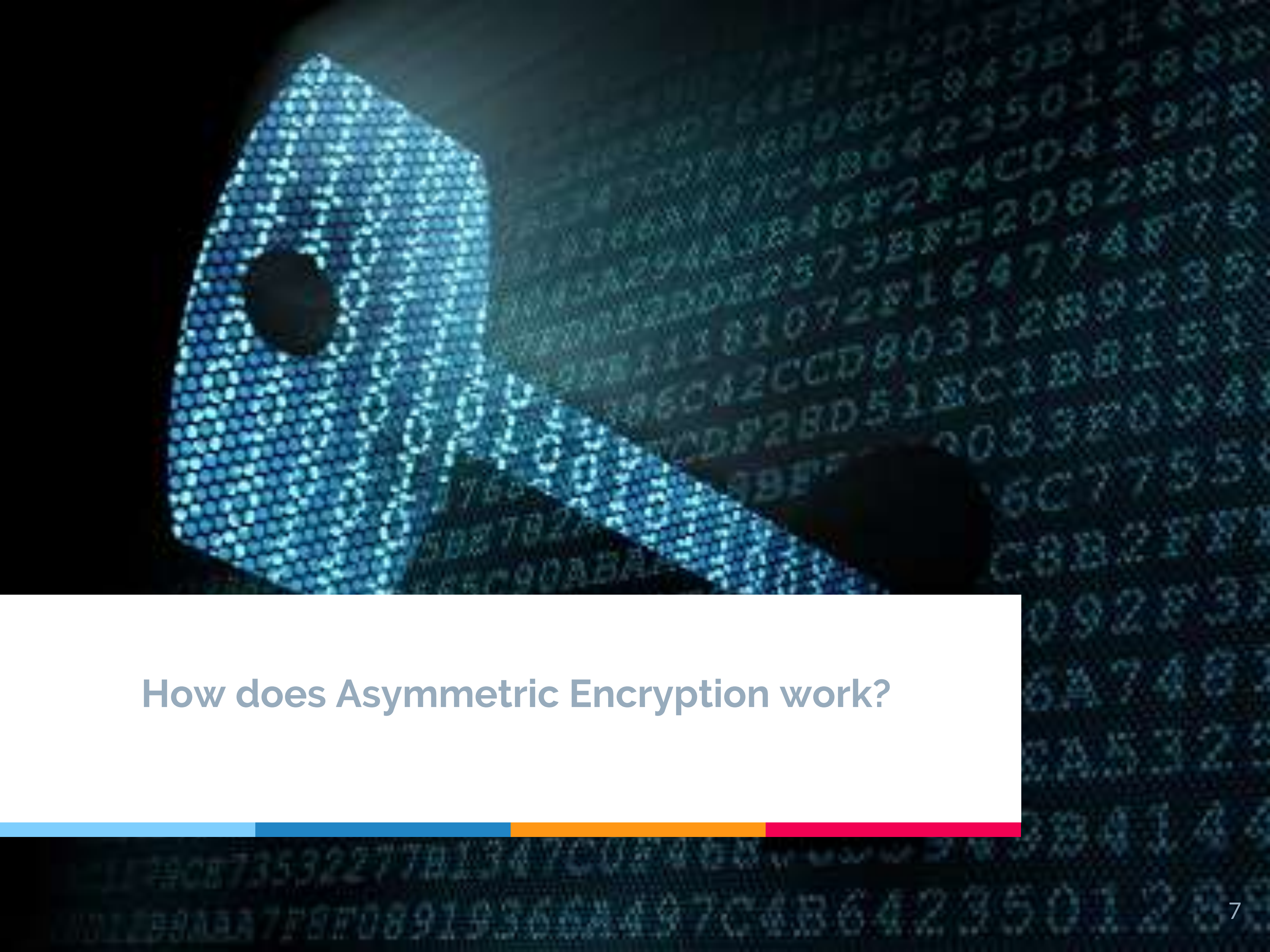
- However, what most people don’t realize is that there are certain types of encryption methods.

Public Key vs Private Key

- Unlike “normal” (**symmetric**) encryption, **Asymmetric Encryption** encrypts and decrypts the data using two separate yet mathematically connected **cryptographic keys**.

- These keys are known as a ‘**Public Key**’ and a ‘**Private Key**.’

- Together, they’re called a ‘**Public and Private Key Pair**.’



How does Asymmetric Encryption work?

Encryption

Public Key

Private Key

Asymmetric Encryption uses two distinct, yet related keys.

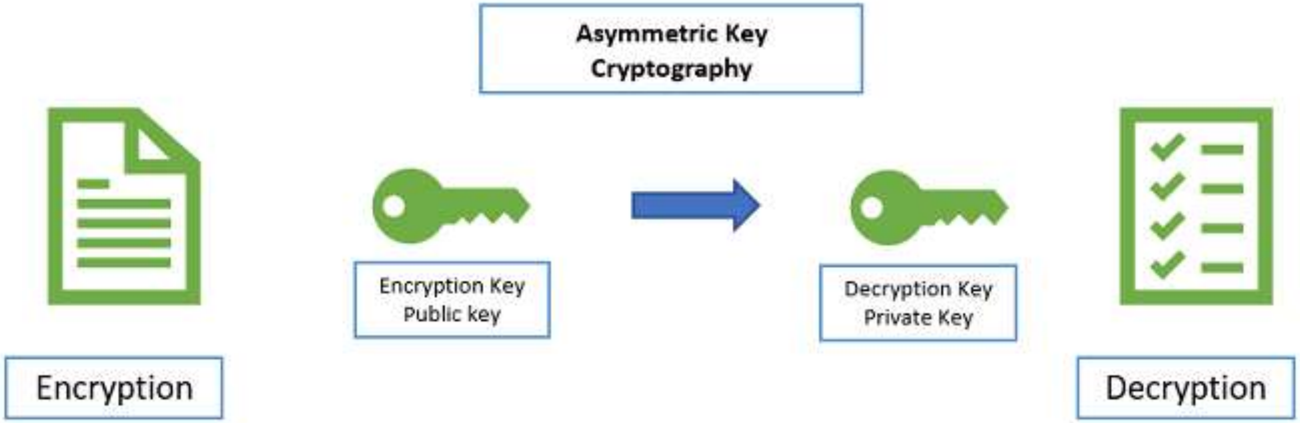
Public Key is used for encryption.

Private Key is used for decryption

As implied in the name, the **Private Key** is intended to be private so that only the authenticated recipient can decrypt the message.

- Pretend you’re a spy agency and you need to devise a mechanism for your agents to report in securely.
- You don’t need two-way communication, they have their orders, you just need regular detailed reports coming in from them.
- Asymmetric encryption would allow you to create public keys for the agents to encrypt their information and a private key back at headquarters that is the only way to decrypt it all.
- This provides an impenetrable form of one-way communication.

Image: Asymmetric Key Cryptography


Asymmetric Key Cryptography
Encryption Key Public key
Decryption Key Private Key
Encryption
Decryption

How are the two keys generated?

At the heart of **Asymmetric Encryption** lies a **cryptographic algorithm**. This algorithm uses a key generation protocol (a kind of mathematical function) to generate a key pair.

Both the keys are mathematically connected with each other.

This relationship between the keys differs from one algorithm to another.

The algorithm is basically a combination of two functions – encryption function and decryption function. To state the obvious, the encryption function encrypts the data and decryption function decrypts it.

This is how Asymmetric Encryption is used in SSL/TLS certificates

▷ In SSL/TLS and other digital certificates, both methods – **Symmetric and Asymmetric – are employed**.

▷ Now, you might be wondering, ‘Why both? Shouldn’t Asymmetric cryptography be used as it’s more secure?’ Granted, it is more secure, but it comes with a pitfall.

▷ A major drawback when it comes to Public Key Cryptography is the computational time.

▷ As the verification and functions are applied from both the sides, it slows down the process significantly.

▷ That’s where Symmetric Encryption comes and saves the day.

- First, when two parties (browser and server in the case of SSL) come across each other, they validate each other's private and public key through Asymmetric Encryption.

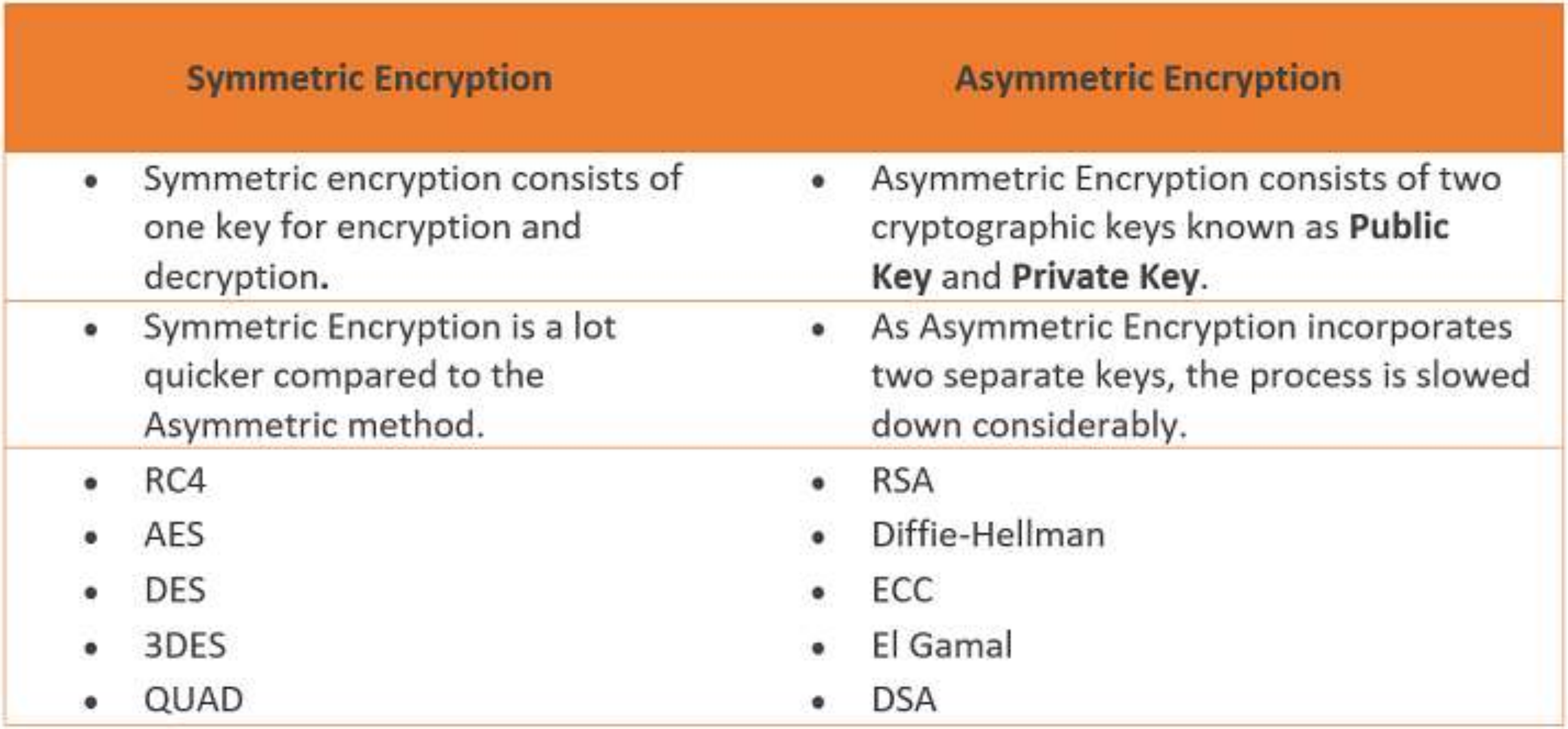
- Once the verification is successful and both know whom they're talking to, the encryption of the data starts – through **Symmetric Encryption.**

- Thereby saving significant time and serving the purposes of confidentiality and data-protection.

- This entire process is called an **SSL/TLS handshake**.

Difference between Symmetric and Asymmetric Encryption

Symmetric Encryption vs Asymmetric Encryption



Symmetric Encryption	Asymmetric Encryption
• Symmetric encryption consists of one key for encryption and decryption.	• Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**.
• Symmetric Encryption is a lot quicker compared to the Asymmetric method.	• As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably.
• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA

You’re using Asymmetric Encryption without even realizing it

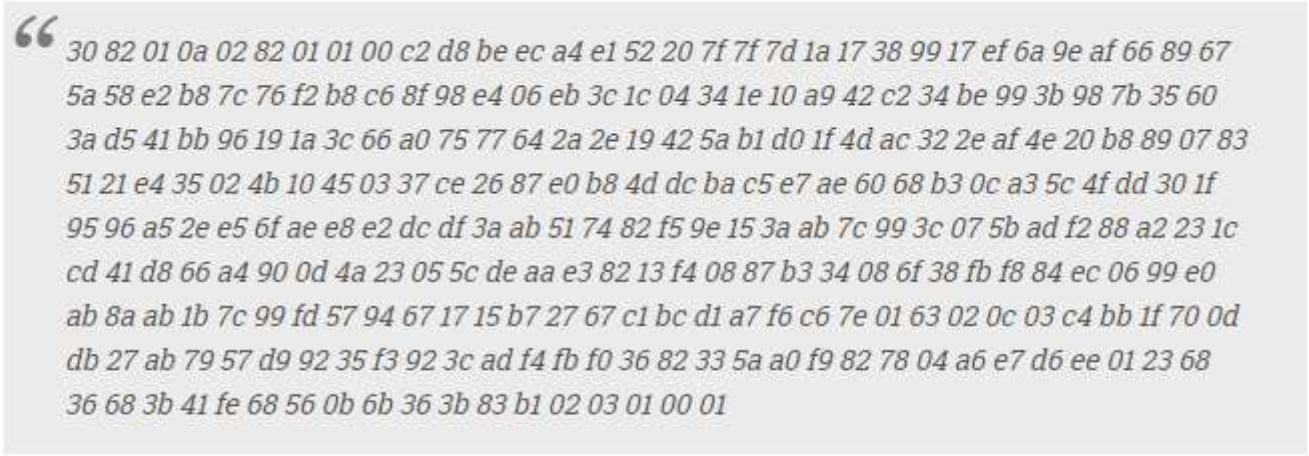
- When you visit any HTTPS website/webpage, your browser establishes Asymmetrically encrypted connection with that website.

- Your browser automatically derives the public key of the SSL/TLS certificate installed on the website (that’s why it’s called ‘Public Key’).

- Do you want to see what it looks like?

- Click the green padlock you see in front of our URL, and go to certificate details.

This is how it’ll look like:



```
30 82 01 0a 02 82 01 01 00 c2 d8 be ec a4 e1 52 20 7f 7f 7d 1a 17 38 99 17 ef 6a 9e af 66 89 67
5a 58 e2 b8 7c 76 f2 b8 c6 8f 98 e4 06 eb 3c 1c 04 34 1e 10 a9 42 c2 34 be 99 3b 98 7b 35 60
3a d5 41 bb 96 19 1a 3c 66 a0 75 77 64 2a 2e 19 42 5a b1 d0 1f 4d ac 32 2e af 4e 20 b8 89 07 83
51 21 e4 35 02 4b 10 45 03 37 ce 26 87 e0 b8 4d dc ba c5 e7 ae 60 68 b3 0c a3 5c 4f dd 30 1f
95 96 a5 2e e5 6f ae e8 e2 dc df 3a ab 51 74 82 f5 9e 15 3a ab 7c 99 3c 07 5b ad f2 88 a2 23 1c
cd 41 d8 66 a4 90 0d 4a 23 05 5c de aa e3 82 13 f4 08 87 b3 34 08 6f 38 fb f8 84 ec 06 99 e0
ab 8a ab 1b 7c 99 fd 57 94 67 17 15 b7 27 67 c1 bc d1 a7 f6 c6 7e 01 63 02 0c 03 c4 bb 1f 70 0d
db 27 ab 79 57 d9 92 35 f3 92 3c ad f4 fb f0 36 82 33 5a a0 f9 82 78 04 a6 e7 d6 ee 01 23 68
36 68 3b 41 fe 68 56 0b 6b 36 3b 83 b1 02 03 01 00 01
```

- So, this key encrypts any information you send to our website during the initial handshake, and our Private Key will decrypt it.
- Do you want to see what our Private Key looks like?
- Here it is

- Oh wait, that’s the key to our office.

- Did we tell you that the Private Key is supposed to be “Private?” Yes, you should NEVER EVER give it to anyone and keep it close to your chest (not literally).

- We recommend storing it at a location where only authorized people have access to it.

- If possible, you should try and save it on a hardware device that’s not connected to your system all the time.

Concluding Words

- Still here? Good.
- We believe that now you (hopefully) know what **Asymmetric Encryption** is and how it protects you from the wrath of **cybercriminals**.
- If you have a website and want to protect it with the same technology.

Thanks for Read, Contact us here.

Blog: cheapsslsecurity.com/blog

Facebook: CheapSSLSecurities

Twitter: SSLSecurity

Google Plus: +Cheapsslsecurity