SSH: Secure Shell Protocol

Linux Session 13

Amna & Mariam Sayed

Session Agenda

01

Introduction

02

Cryptography

03

Secure Shell

04

Let’s Play!

01

Introduction

Networking recap, and motive for security.

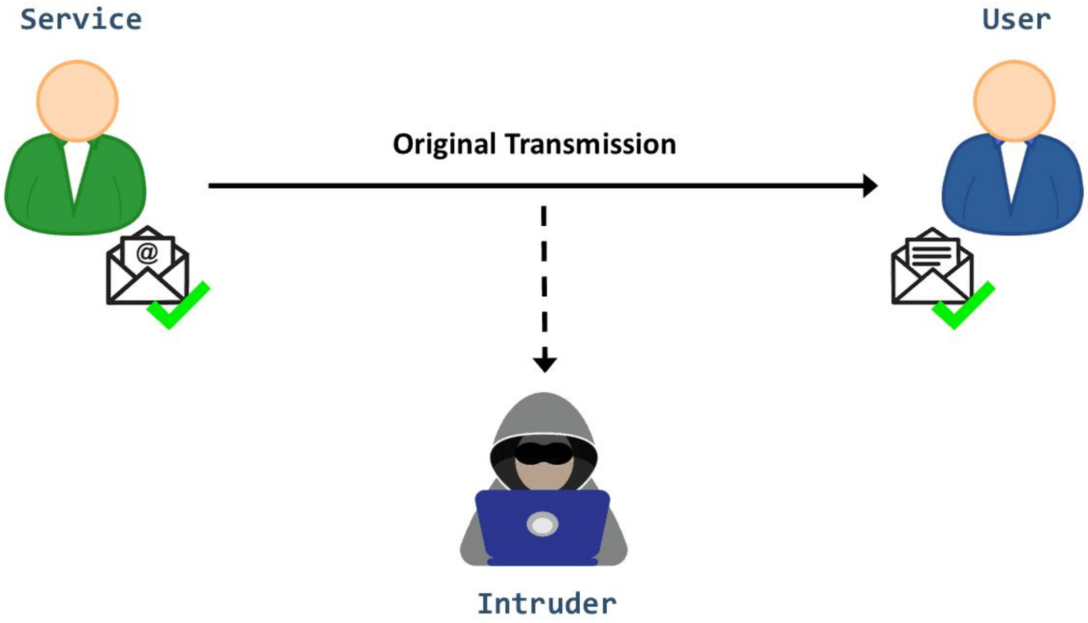
Let's Recall Networking

- The internet is a **network of networks**, connecting end devices via switches and routers.
- Any form of communication is data transmission, and any data is represented as zeroes and ones.

Let's Recall Networking

- These bits are converted into signals and transmitted along a medium, which can be wired or wireless.
- In our current mental model, the data is transmitted as-is **without protection**.
- What if it got intercepted during transmission?

Let’s Recall Networking



How can we protect our data during transmission?

02

Cryptography

What is Cryptography?

- In cryptography, we aim to exchange information securely between a sender and a recipient.
- This ensures that even if the data is intercepted by a third party, they will gain no meaningful information from it.

What is Cryptography?

- In a nutshell, this is done by converting the original data (**plaintext**) to a form that only the recipient can understand (**ciphertext**) before transmitting it.
- This conversion is called **encryption**.
- The reverse process is called **decryption**.

Important Assumption

- We will assume the algorithm and its details is known.
- *“A cryptographic system should be secure even if everything about the system, except for the key, is public knowledge.”*
- This is called **Kerckhoffs's Principle.**

Types of Cryptography

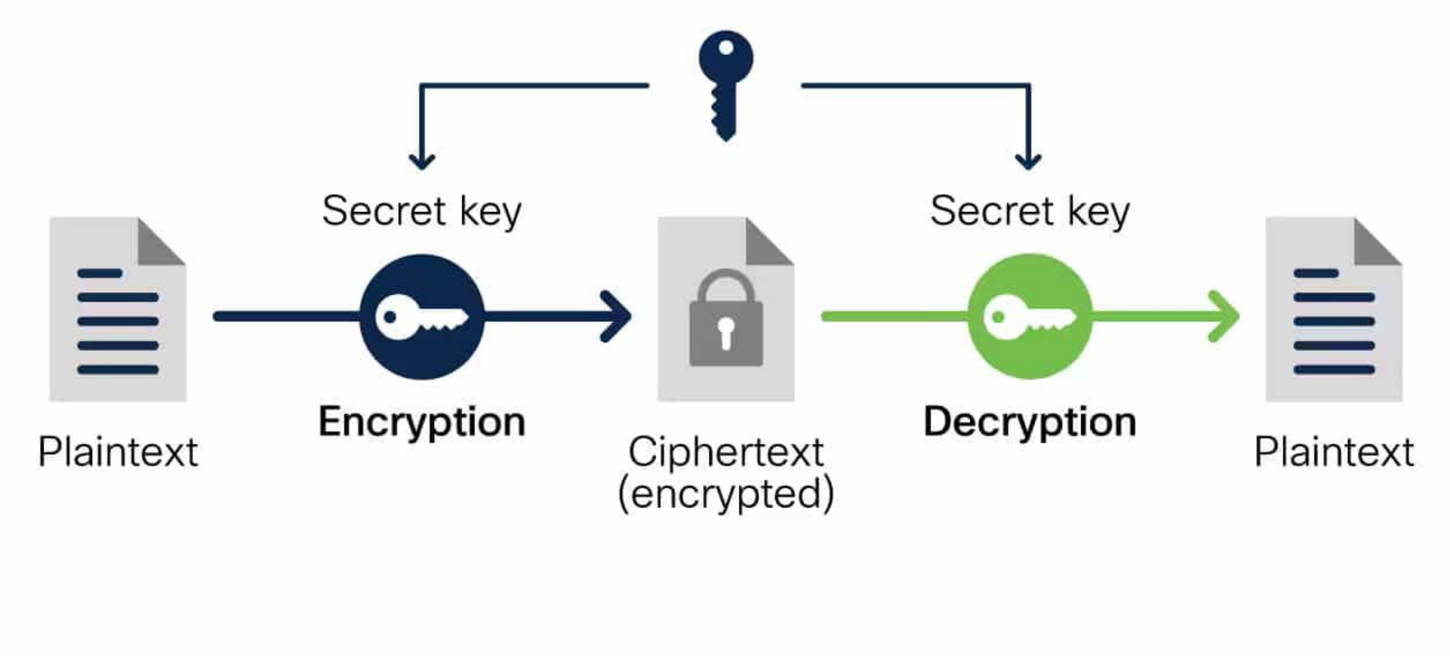
Symmetric

Same key for encryption/ decryption

Asymmetric

Different keys for encryption/ decryption

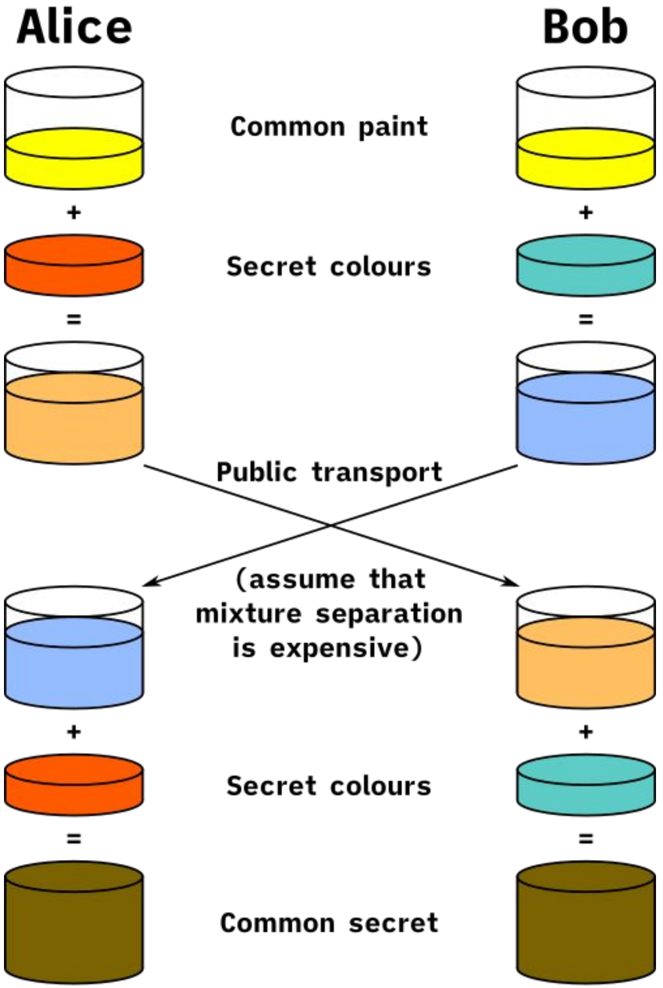
Symmetric Key Cryptography



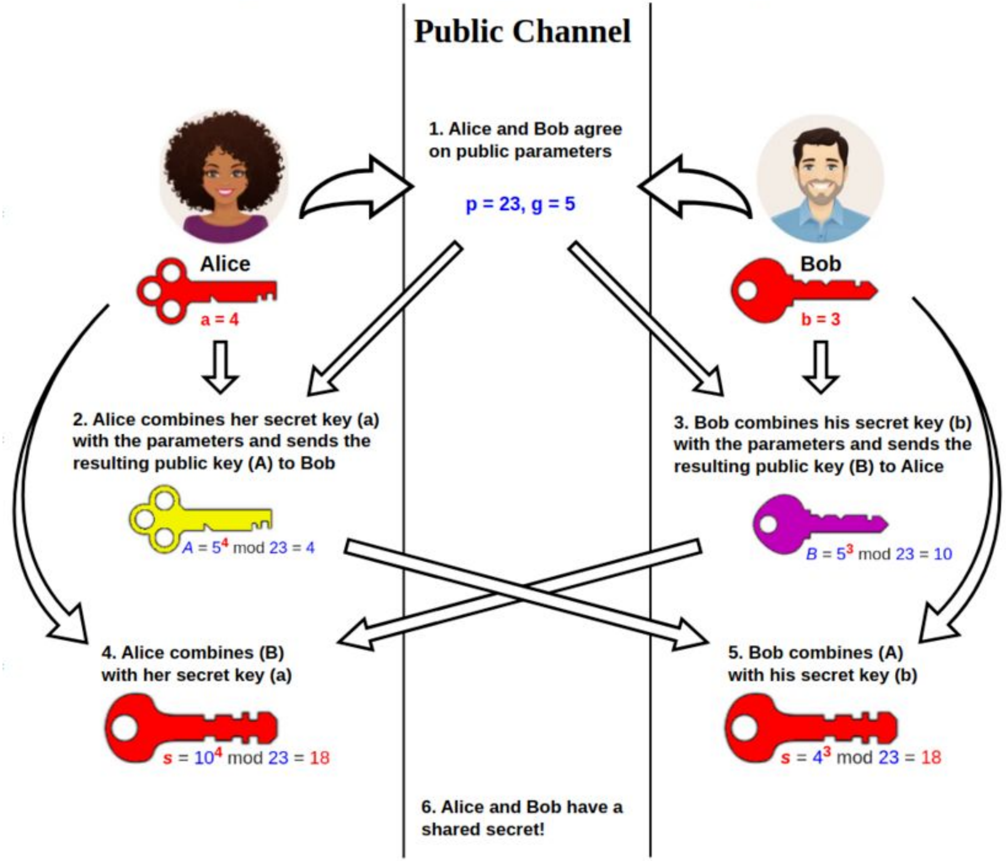
How can we exchange the encryption key?

Diffie-Hellman Key Exchange

Using colors instead of large numbers is a helpful analogy.



Diffie-Hellman Key Exchange



Public Channel

1. Alice and Bob agree on public parameters

$p = 23, g = 5$

Alice

$a = 4$

Bob

$b = 3$

2. Alice combines her secret key (a) with the parameters and sends the resulting public key (A) to Bob

$A = 5^4 \bmod 23 = 4$

3. Bob combines his secret key (b) with the parameters and sends the resulting public key (B) to Alice

$B = 5^3 \bmod 23 = 10$

4. Alice combines (B) with her secret key (a)

$s = 10^4 \bmod 23 = 18$

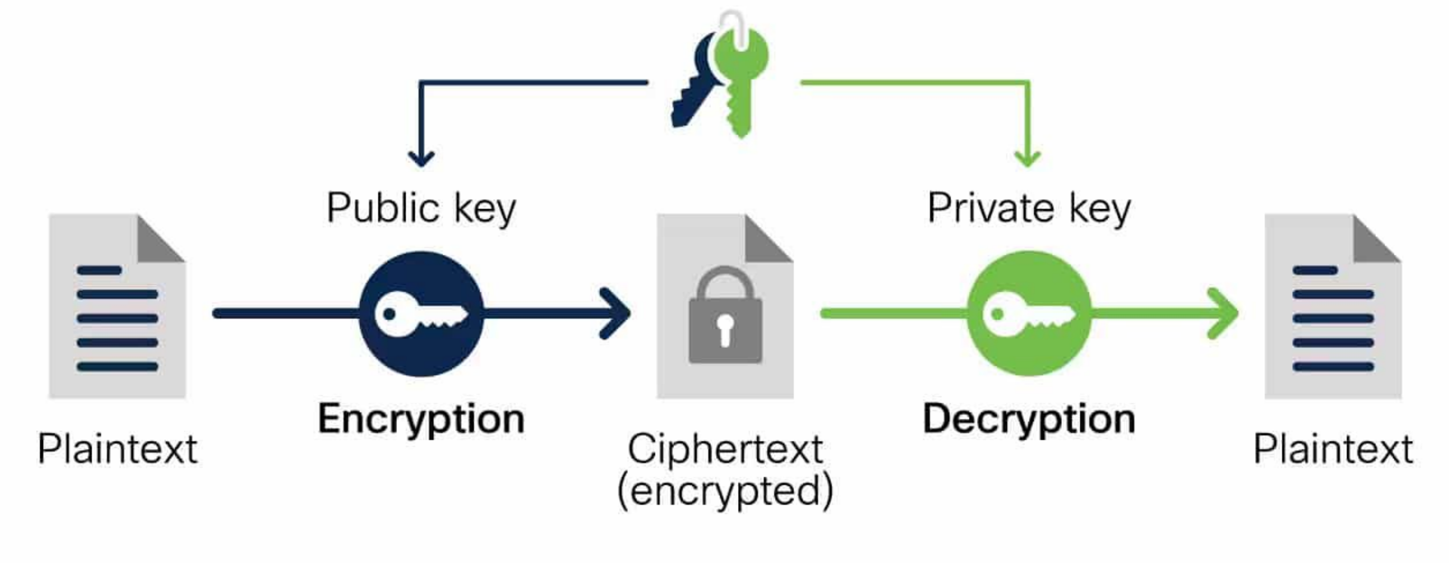
5. Bob combines (A) with his secret key (b)

$s = 4^3 \bmod 23 = 18$

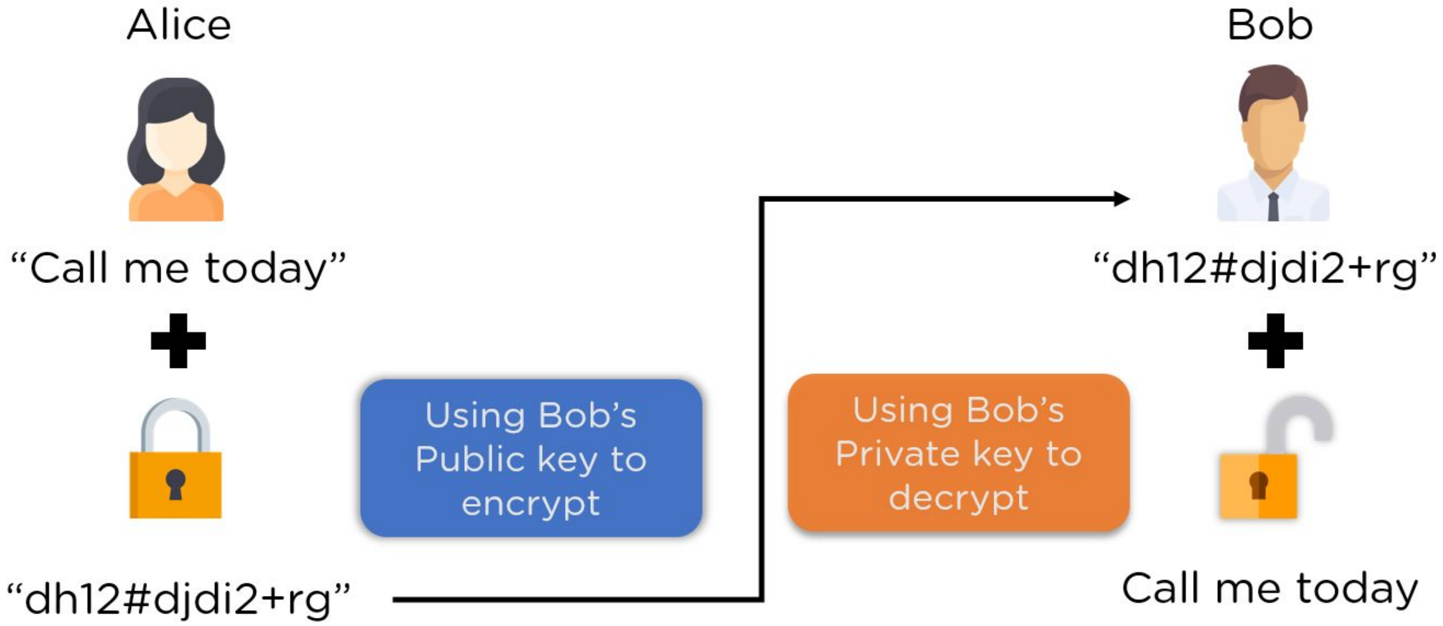
6. Alice and Bob have a shared secret!

Asymmetric Key Cryptography

Also called public-key cryptography.



Asymmetric Key Cryptography



Alice

“Call me today”

“dh12#djdi2+rg”

Using Bob’s Public key to encrypt

Using Bob’s Private key to decrypt

Bob

“dh12#djdi2+rg”

Call me today

03

Secure Shell (SSH)

Secure remote connections in action

Secure Shell (SSH)

- SSH is a cryptographic network protocol that enables **secure** connection over **unsecured** networks.
- It has many use cases, most notably **remote administration.**

Secure Shell (SSH)

We have three main questions we want to answer:

1. How can the client authenticate itself to the server?
2. How to encrypt the transmitted data?
3. How to exchange the encryption key securely?

1. How can the client authenticate itself to the server?

- Password authentication can be used, or
- A **public-key encryption algorithm**

SSH Public-Key Authentication

- Client generates public and private key
- Client uploads its public key to the server
- Client requests connection using SSH
- If the server identifies the client's public key, it uses it to encrypt a message and sends it as a *challenge*

SSH Public-Key Authentication

- The client uses its private key to decrypt the challenge, and performs some calculations before sending it back to the server.
- If the client succeeds, the server agrees to open the connection
- If not, the server refuses the connection

2. How to encrypt the transmitted data?

- Symmetric encryption algorithms are used here.
- They are faster than public-key algorithms.
- However, we immediately run into the second problem...

3. How to exchange the encryption key securely?

- Sending it over the network would bring us back to square one.
- A key exchange algorithm is used so that the two parties can generate the same key independently and securely.
    - For example: **Diffie-Hellman Algorithm**

Key Generation

Generate SSH keys interactively

```
ssh-keygen
```

Copy the given key to the remote

```
ssh-copy-id -i path/to/key user@host
```

SSH Command

Connecting via SSH	`ssh [options] user@host`
Using private key	`-i path/to/private/key`
Using a specific port	`-p port_number`

SSH Config Files

```
~/.ssh/config
```

```
~/.ssh/authorized_keys
```

04

Let’s Play!

Put your skills to the test through Bandit CTF.

OverTheWire Bandit

Congratulations

You are now armed with SSH!

Session Task

Complete the Bandit wargame, and submit a screenshot from the last level.

Thank You!