

The trust in the digital world

Introduction



Can you trust me?

- Make sure you are communicating with the right person
- Ensure that no one else is involved in the exchange

How can you trust a person who's not physically in front of you?

Expected communication



Alice

« Hi, I'm Alice! »



« Hey Alice, I'm Bob! »



Bob

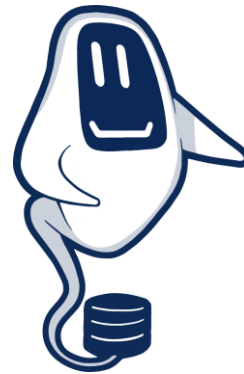
Man-in-the-middle



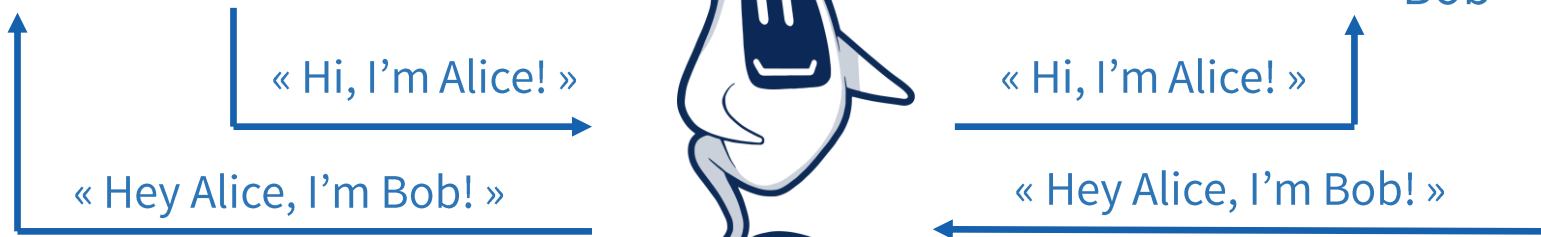
Alice



Bob



Eve

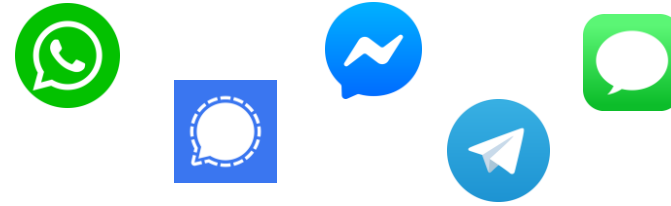


End-to-end encryption

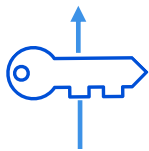
Symmetric keys



End-to-end encryption



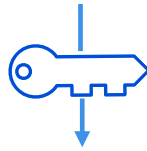
« Hey Alice, I'm Bob! »



```
89C35F5CA393FF9392
5C24D9B7070A5AD42
Encrypted message 2
```



« Hi, I'm Alice! »

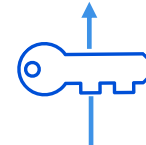


```
0E9490A68F7AD5C11E
A794858A4045473491
Encrypted message 1
```



Symmetric key

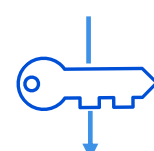
« Hi, I'm Alice! »



```
0E9490A68F7AD5C11E
A794858A4045473491
Encrypted message 1
```



« Hey Alice, I'm Bob! »

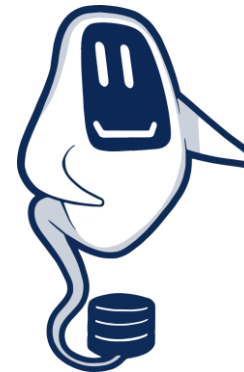


```
89C35F5CA393FF9392
5C24D9B7070A5AD42
Encrypted message 2
```

Alice

```
0E9490A68F7AD5C11E
A794858A4045473491
Encrypted message 1
```

```
89C35F5CA393FF9392
5C24D9B7070A5AD42
Encrypted message 2
```



Eve

Bob

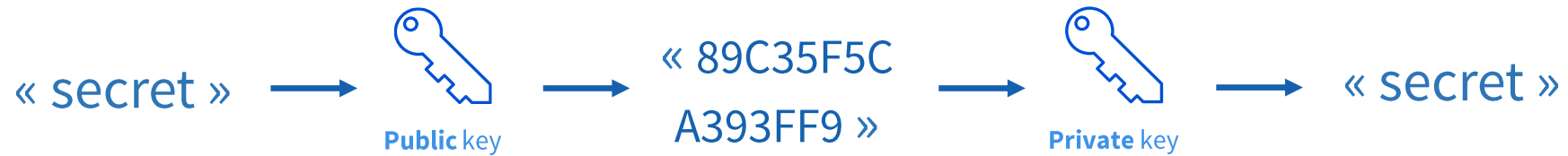
```
0E9490A68F7AD5C11E
A794858A4045473491
Encrypted message 1
```

```
89C35F5CA393FF9392
5C24D9B7070A5AD42
Encrypted message 2
```



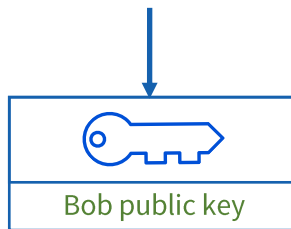
End-to-end encryption

Asymmetric key pairs



Trust : Asymmetric key pairs

« Here's my secret »



« 0E9490A68
F7AD5C11E
A794858A4
045473491 »



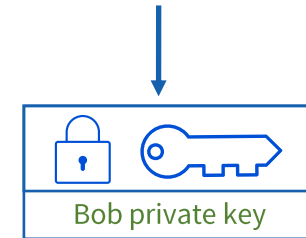
Alice

« 0E9490A68
F7AD5C11E
A794858A4
045473491 »



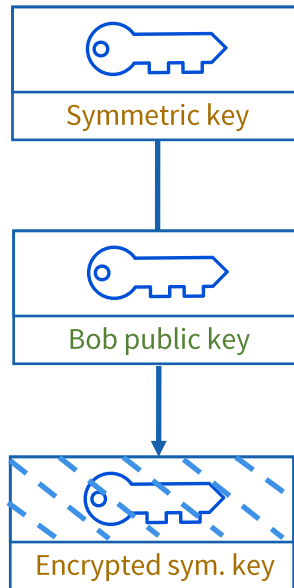
Bob

« 0E9490A68
F7AD5C11E
A794858A4
045473491 »



« Here's my secret »

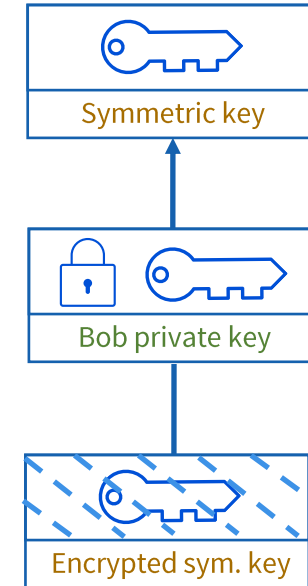
Trust : Asymmetric key pairs



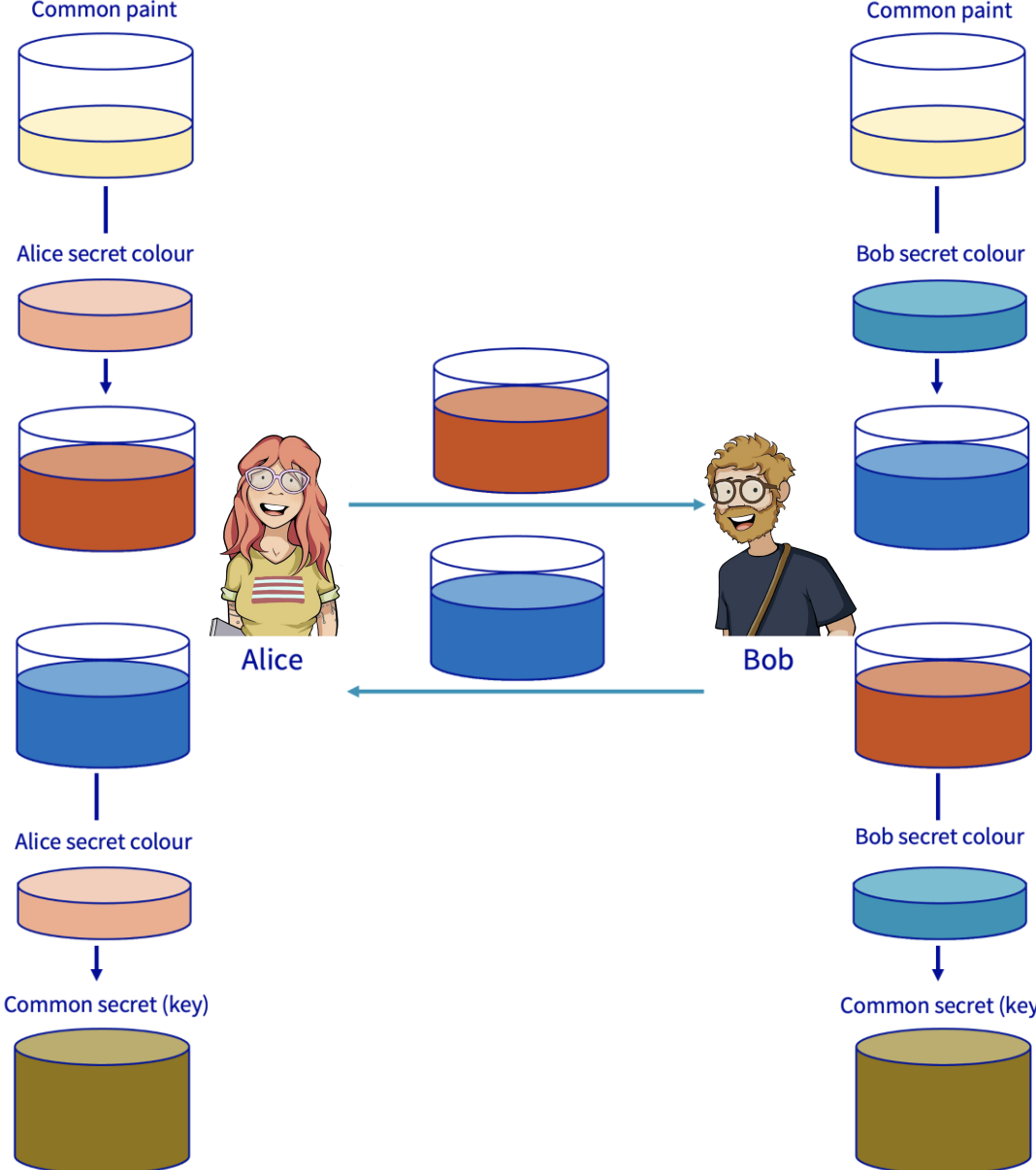
Alice



Bob



Trust : Diffie-Hellman exchange

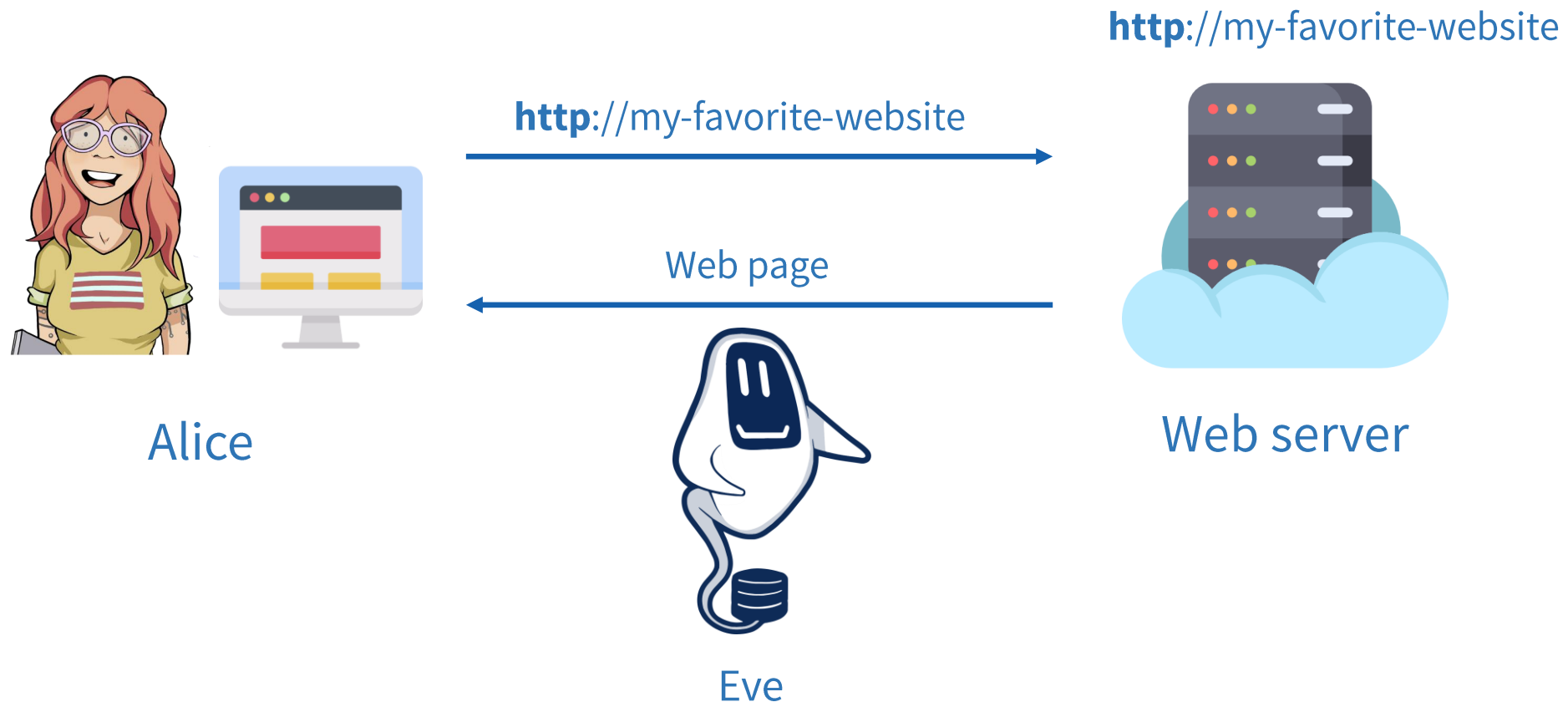


Trust in the web world with TLS

HTTPS

HyperText Transfer Protocol **Secure**

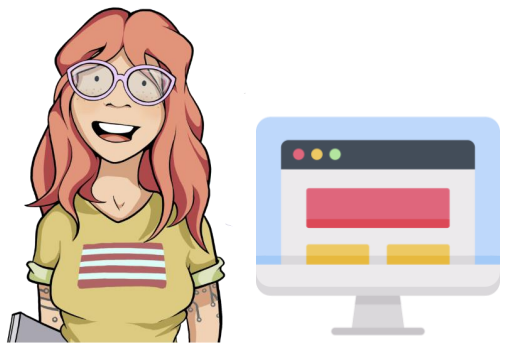
Trust in the web world with TLS



Trust in the web world with TLS

« I'm my-favorite-website! »

 <https://my-favorite-website>



Alice

<https://my-favorite-website>

Web page



Web server



Certificate

Trusted third party



Certificate authority

« Yes, it's my-favorite-website. I checked. »

Trust in the web world with TLS



Certificate

- Authenticity
- Encryption
- Integrity



Trust in the web world with TLS

- Domain Common Name
- CA Signature
- CA Public Key



End-entity
Certificate

Signed by



Intermediate
CA Certificate

Signed by



Root CA
Certificate

Trust in the web world with TLS

⚠ Not Secure | https://



Your connection is not private

Attackers might be trying to steal your information from (for example, passwords, messages or credit cards). [Learn more](#)

NET::ERR_CERT_COMMON_NAME_INVALID

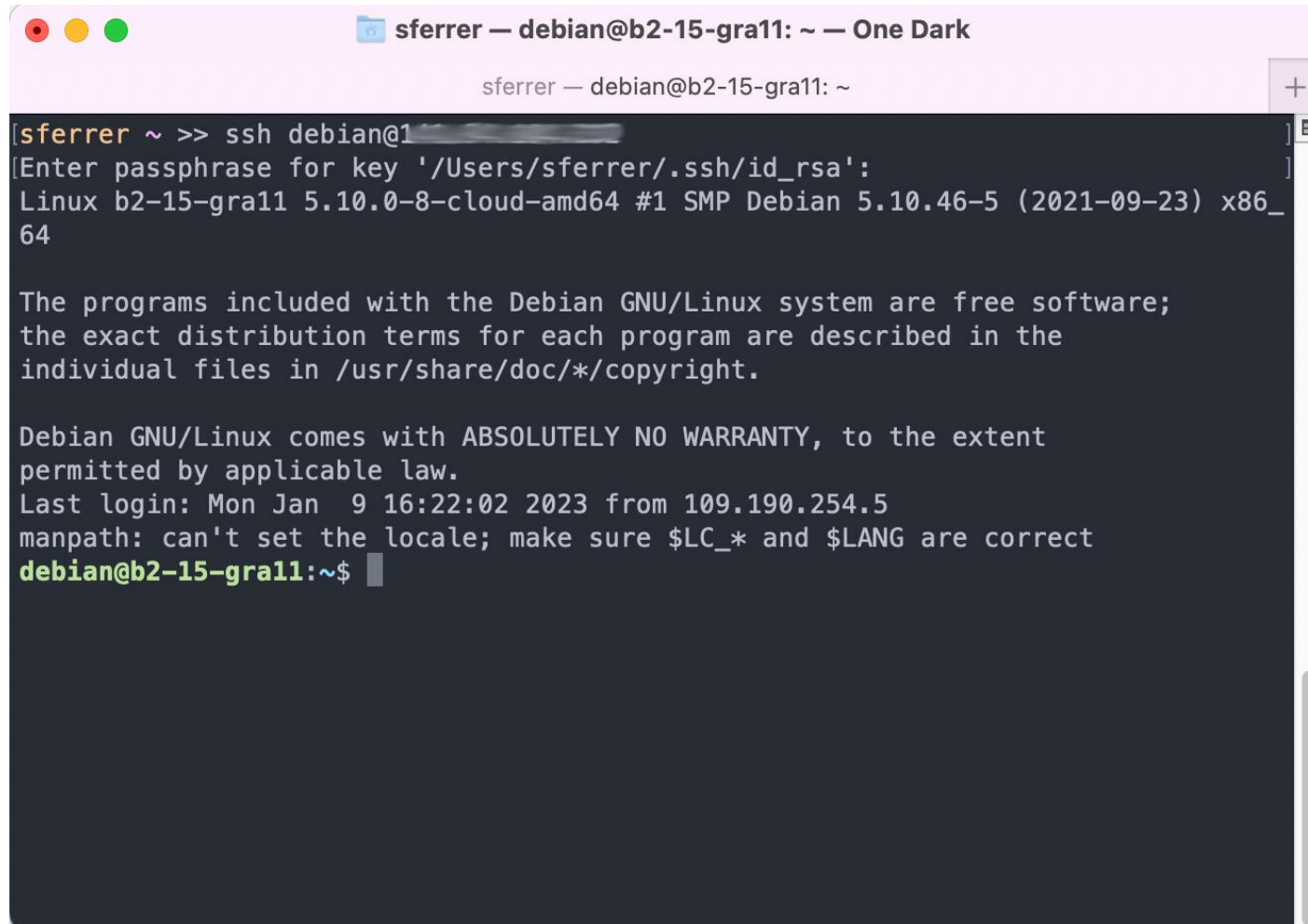


To get Chrome's highest level of security, [turn on enhanced protection](#)

Advanced

Back to safety

Trust with SSH

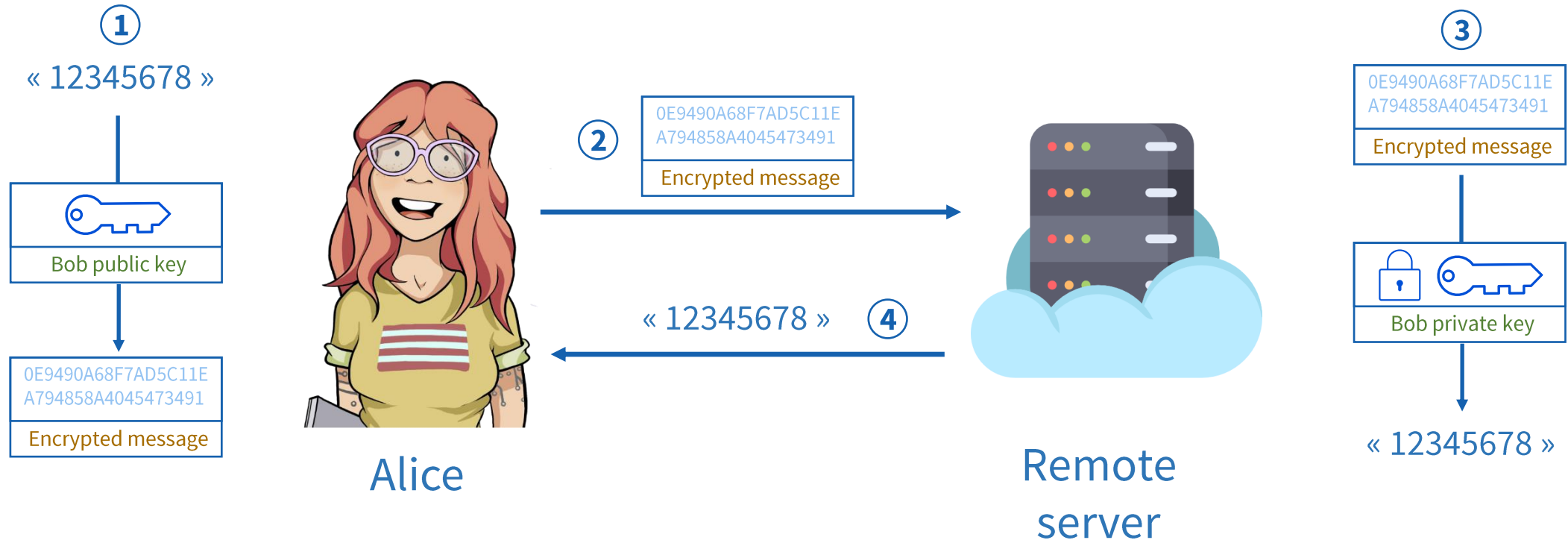


```
sferrer — debian@b2-15-gra11: ~ — One Dark
sferrer — debian@b2-15-gra11: ~
[sferrer ~ >> ssh debian@1[redacted]
[Enter passphrase for key '/Users/sferrer/.ssh/id_rsa':
Linux b2-15-gra11 5.10.0-8-cloud-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_
64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jan  9 16:22:02 2023 from 109.190.254.5
manpath: can't set the locale; make sure $LC_* and $LANG are correct
debian@b2-15-gra11:~$
```

Trust with SSH



References

Encryption:

- <https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/>
- https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

TLS:

- [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785811\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785811(v=ws.10))
- https://en.wikipedia.org/wiki/Transport_Layer_Security
- <https://letsencrypt.org/documents/isrg-cp-v3.1/>
- <https://www.keyfactor.com/blog/certificate-chain-of-trust/>
- https://en.wikipedia.org/wiki/OCSP_stapling
- https://en.wikipedia.org/wiki/X.509#Certificate_chains_and_cross-certification
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>
- <https://security.stackexchange.com/questions/119364/how-can-i-detect-https-inspection>
- <https://learn.microsoft.com/en-us/windows-hardware/drivers/install/certificate-stores>

SSH:

- <https://www.digitalocean.com/community/tutorials/ssh-essentials-working-with-ssh-servers-clients-and-keys>
- <https://security.stackexchange.com/questions/182804/how-does-ssh-know-which-public-key-to-use-from-authorized-keys>
- <https://www.rfc-editor.org/rfc/rfc4252.html>
- https://en.wikipedia.org/wiki/Secure_Shell
- <https://docs.microsoft.com/en-us/azure/devops/repos/git/use-ssh-keys-to-authenticate?view=azure-devops>



Kimi, my cat



sebferrer



seb-ferrer



<https://blog.kimi.ovh>



A more detailed blog
post about federated
identities here