Basics of Cryptography and Applications

ÖNDER GÖRMEZ

Agenda

I. Background - Experience
II. Cryptographic Hash Functions
III. Symmetric Key Cryptography
IV. Asymmetric Key Cryptography
V. Cryptography Applications
VI. References
VII. Q & A

Agenda

I. **Background - Experience**

II. **Cryptographic Hash Functions**

III. **Symmetric Key Cryptography**

IV. **Asymmetric Key Cryptography**

V. **Cryptography Applications**

VI. **References**

VII. **Q & A**

Background - Experience

I have over 8 years of experience in the software/hardware development industry.

Skills;

- Programming Languages;
  - C/C++
  - Java/C#
  - JavaScript
  - Python
  - Scala

- Project Management
  - Agile Software Development
  - Software Project Management
  - Hardware Project Management
  - Requirement Analysis

Agenda

I. Background - Experience

II. Cryptographic Hash Functions

III. Symmetric Key Cryptography

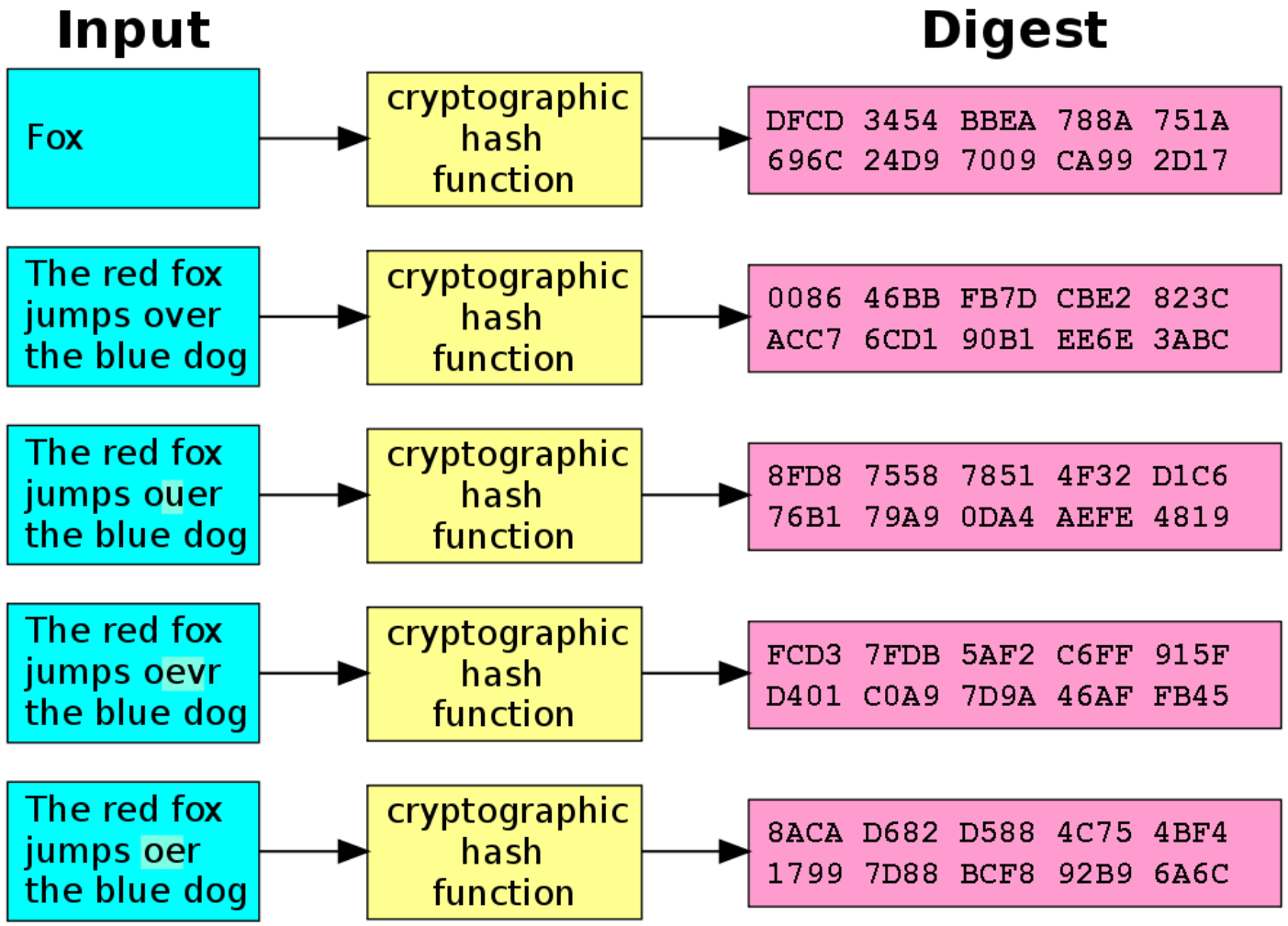
IV. Asymmetric Key Cryptography

V. Cryptography Applications

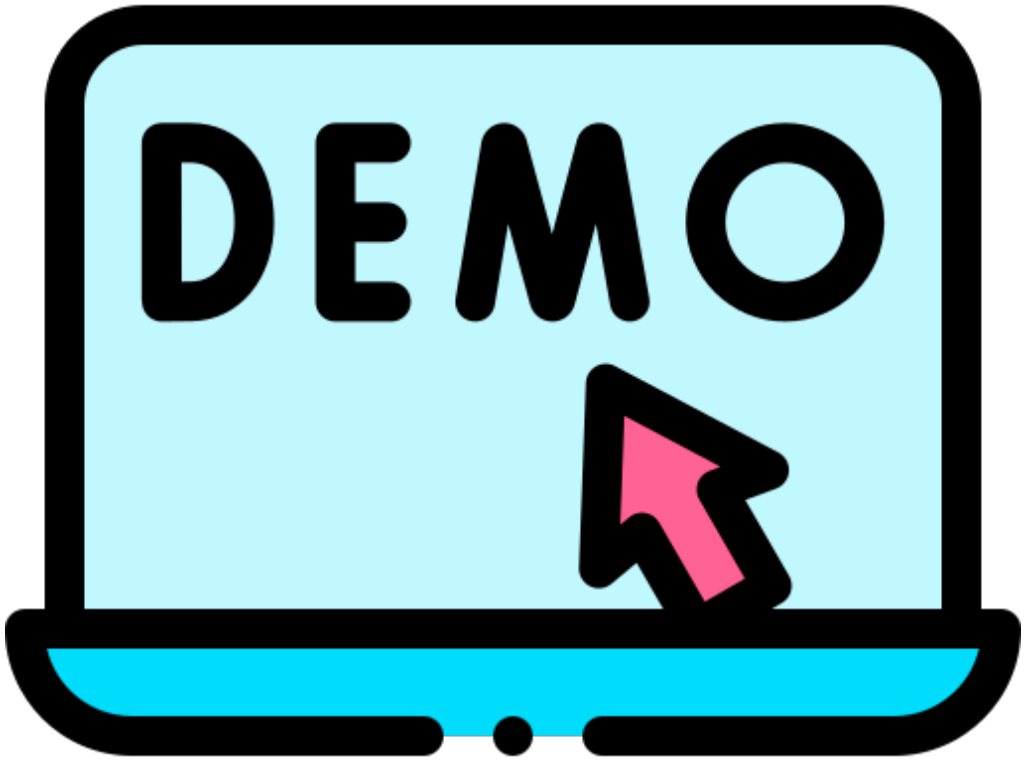
VI. References

VII. Q & A

Cryptographic Hash Functions



Cryptographic Hash Functions



Agenda

I. Background - Experience

II. Cryptographic Hash Functions

III. Symmetric Key Cryptography

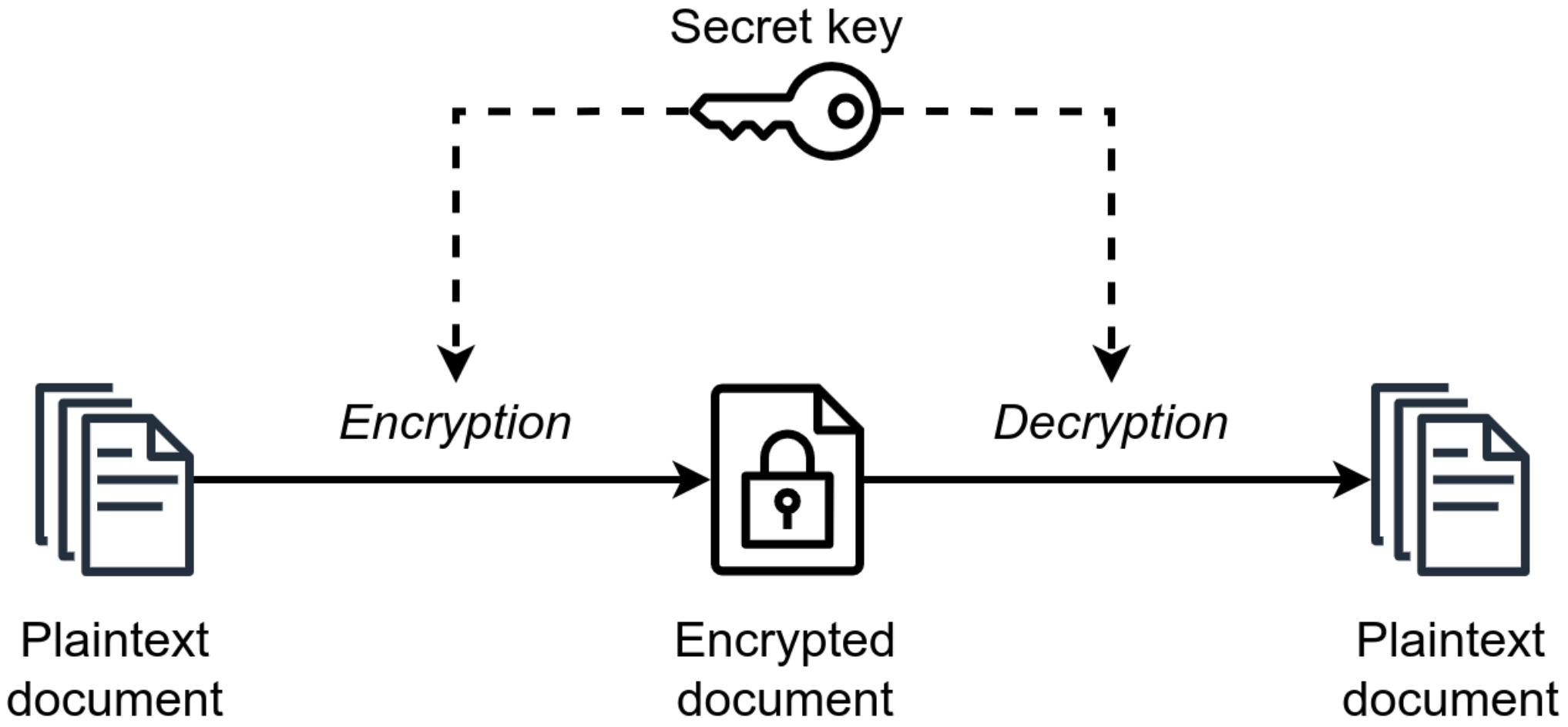
IV. Asymmetric Key Cryptography

V. Cryptography Applications

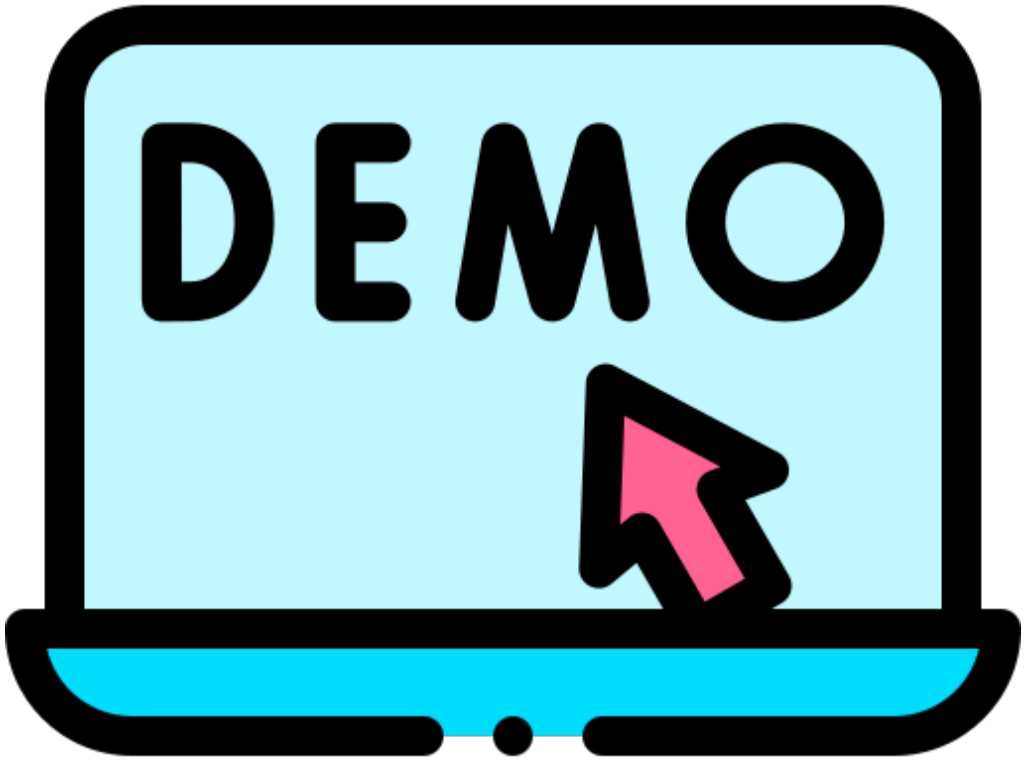
VI. References

VII. Q & A

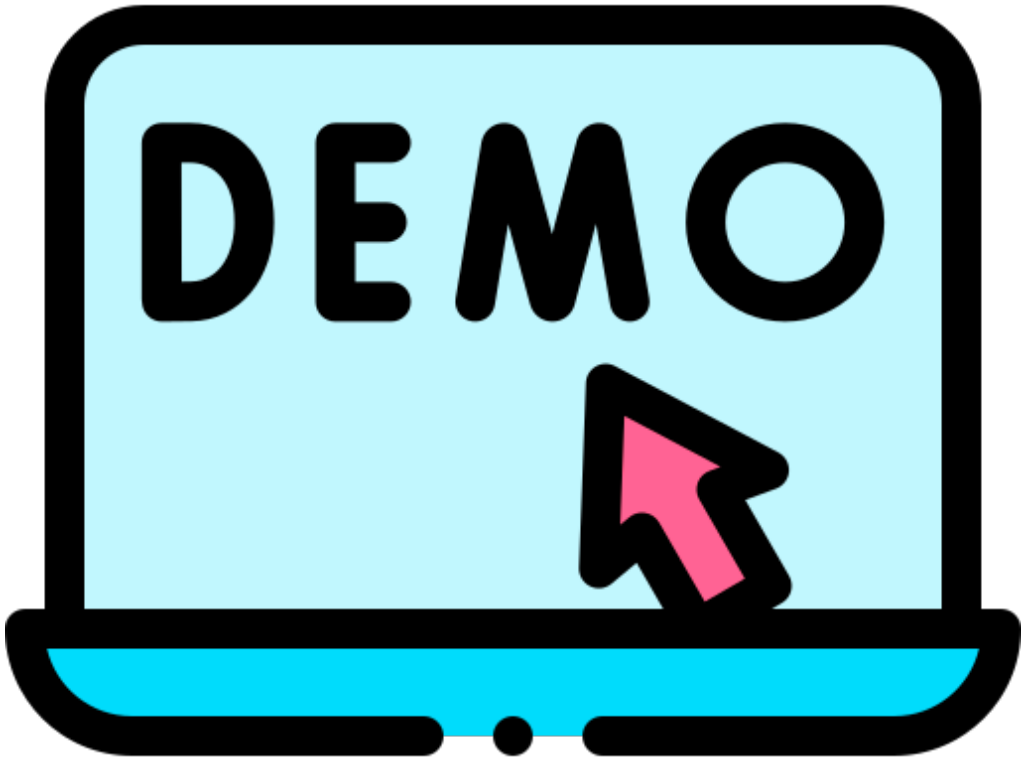
Symmetric Key Cryptography



Demo - DES Encryption/Decryption



Demo - AES Encryption/Decryption



Agenda

I. Background - Experience

II. Cryptographic Hash Functions

III. Symmetric Key Cryptography

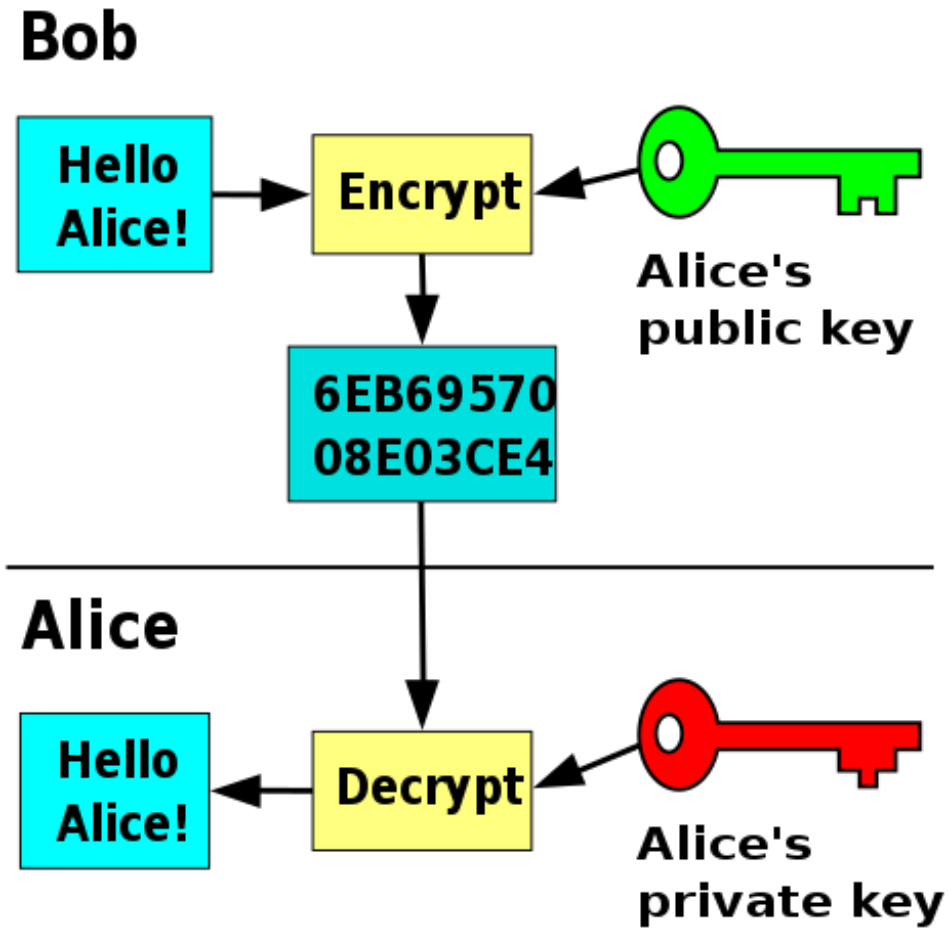
IV. Asymmetric Key Cryptography

V. Cryptography Applications

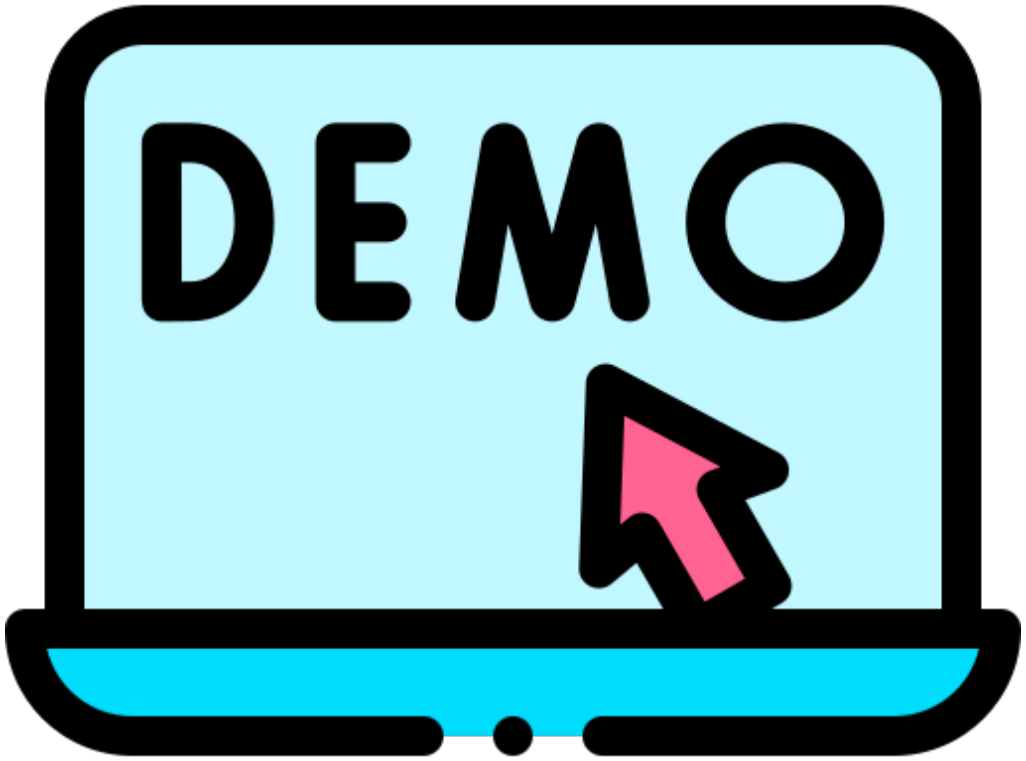
VI. References

VII. Q & A

Asymmetric Key Cryptography



Demo - RSA Encryption/Decryption



Agenda

I. Background - Experience

II. Cryptographic Hash Functions

III. Symmetric Key Cryptography

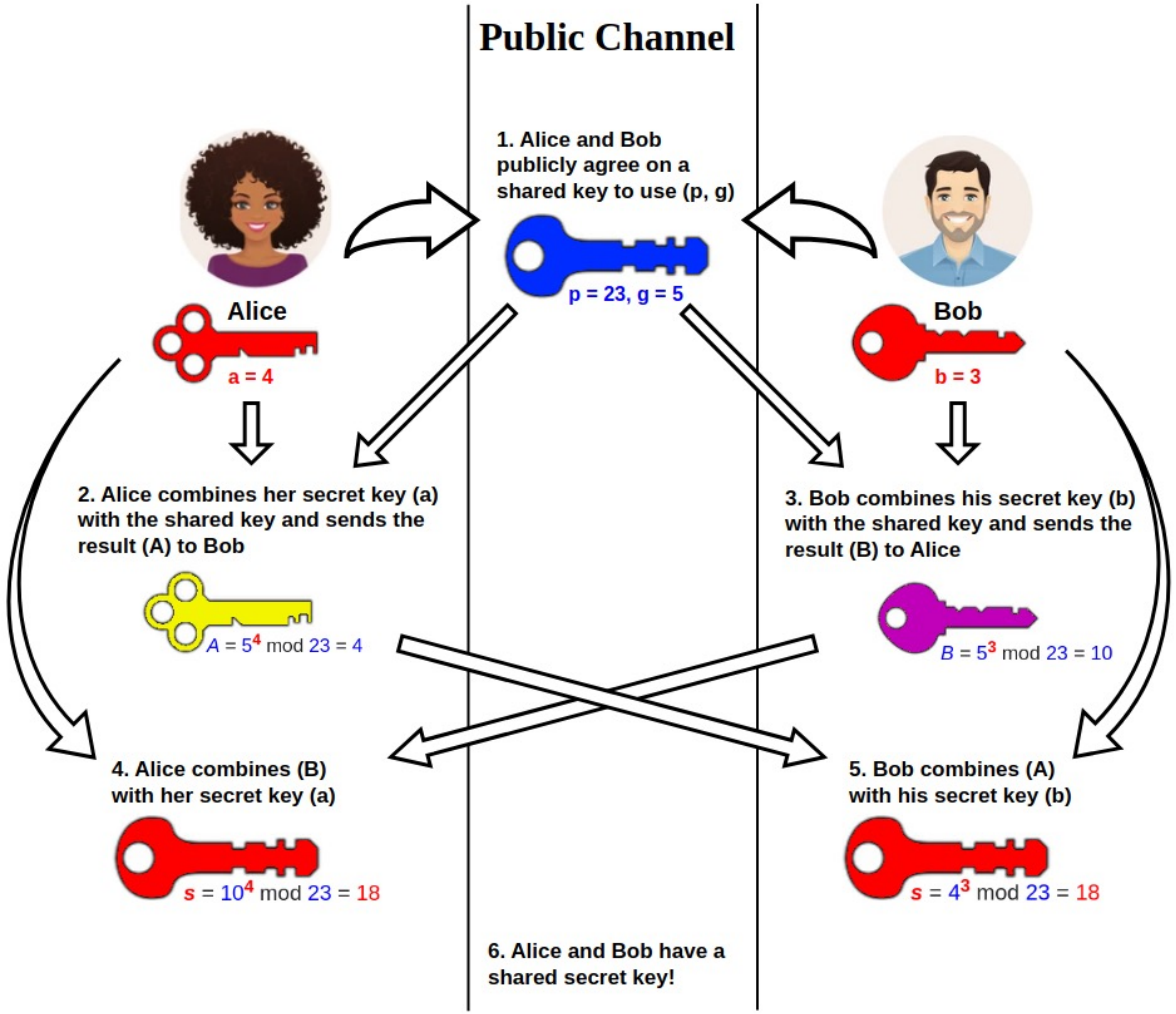
IV. Asymmetric Key Cryptography

V. Cryptography Applications

VI. References

VII. Q & A

Cryptography Applications - Diffie–Hellman Key Exchange



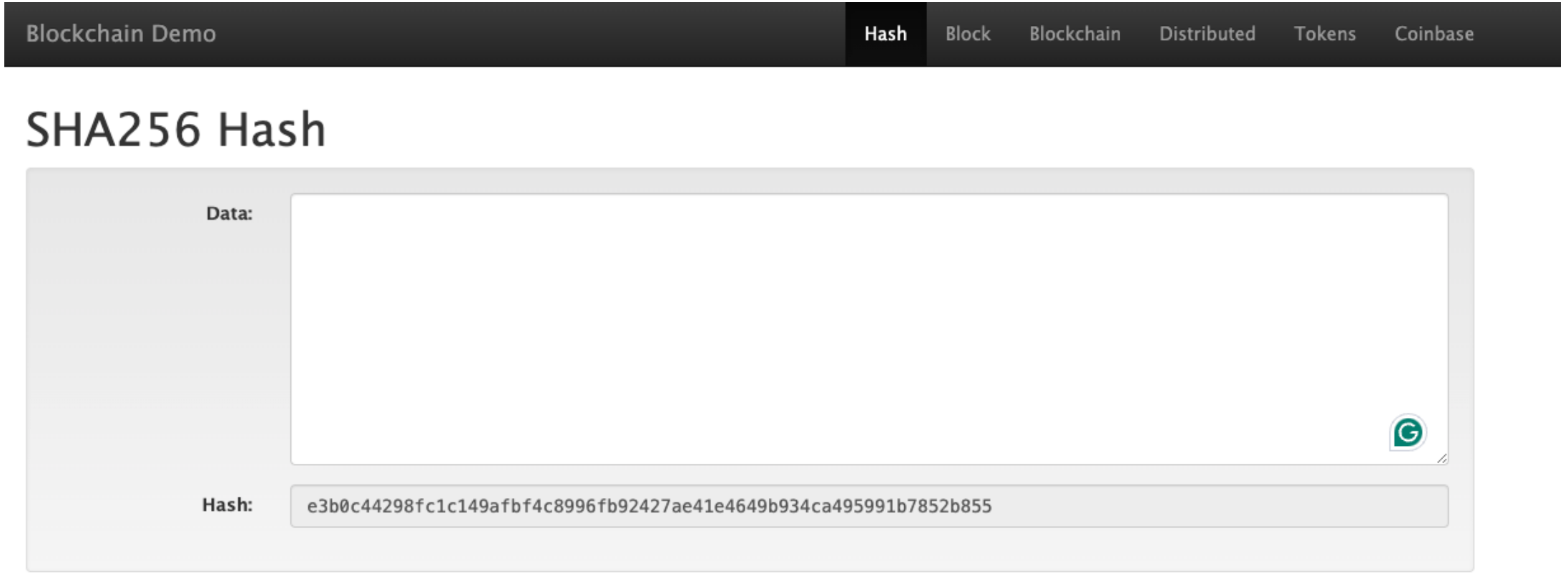
Cryptography Applications - Git SSH Key

```
ssh-keygen -t rsa -C "ondergormez@gmail.com"
ls ~/.ssh/
cat ~/.ssh/id_rsa.pub

ssh-keygen -t ed25519 -C "ondergormez@gmail.com"
ls ~/.ssh/
cat ~/.ssh/id_ed25519.pub

openssl genrsa -out private_key.pem 2048
cat private_key.pem
openssl rsa -in key.pem -outform PEM -pubout -out public_key.pem
cat public_key.pem
```

Cryptography Applications - Bitcoin Mining



Source: https://andersbrownworth.com/blockchain/hash

Visual Demo: https://andersbrownworth.com/blockchain/public-private-keys/

Agenda

I. Background - Experience

II. Cryptographic Hash Functions

III. Symmetric Key Cryptography

IV. Asymmetric Key Cryptography

V. Cryptography Applications

VI. References

VII. Q & A

References

[1] https://en.wikipedia.org/

[2] https://andersbrownworth.com/blockchain/public-private-keys/

Agenda

I. Background - Experience

II. Cryptographic Hash Functions

III. Symmetric Key Cryptography

IV. Asymmetric Key Cryptography

V. Cryptography Applications

VI. References

VII. Q & A

Basics of Cryptography and Applications

THANK YOU FOR LISTENING…