

# 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**

# Basics of Cryptography and Applications

## 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

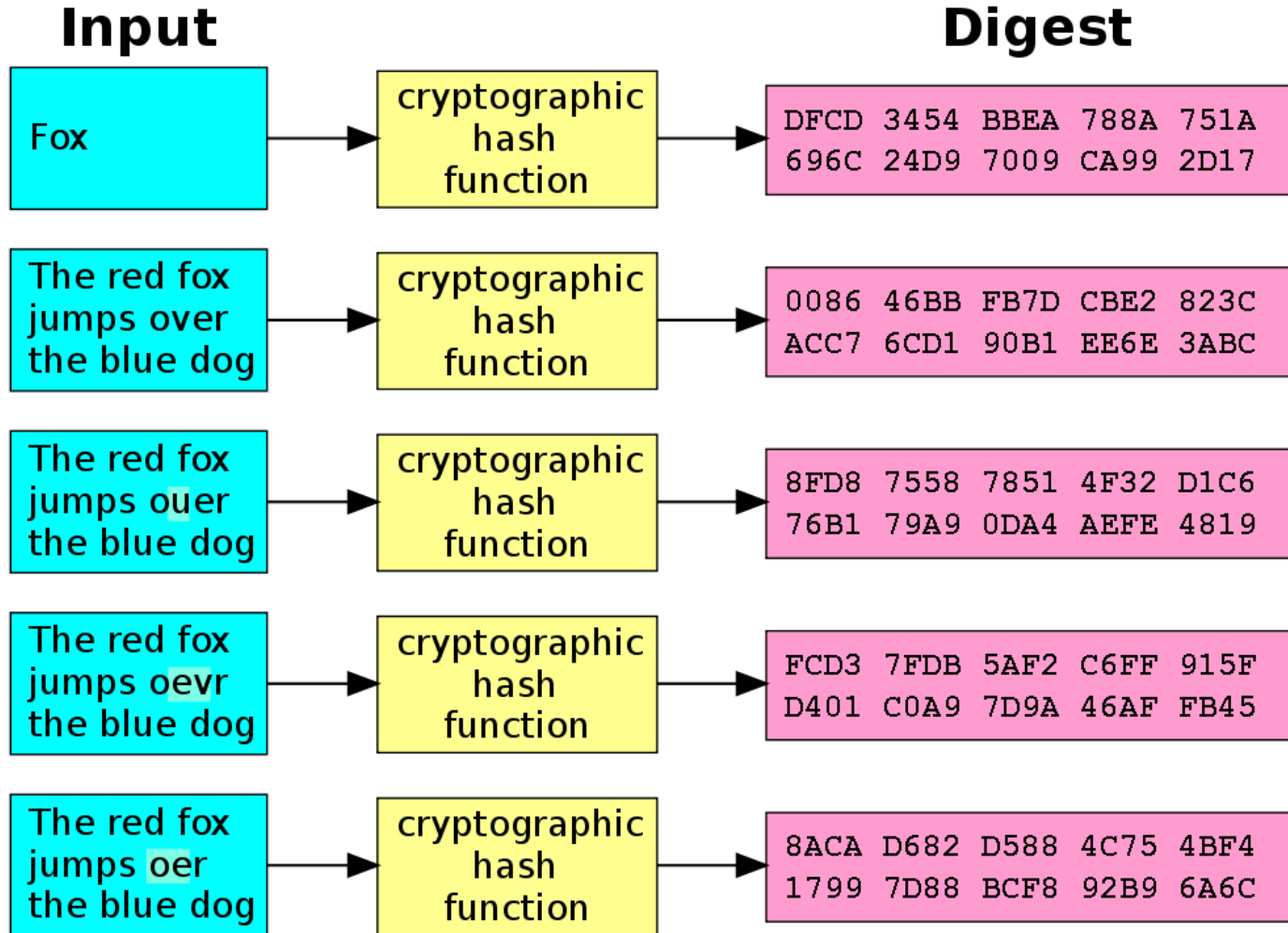


# Agenda

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

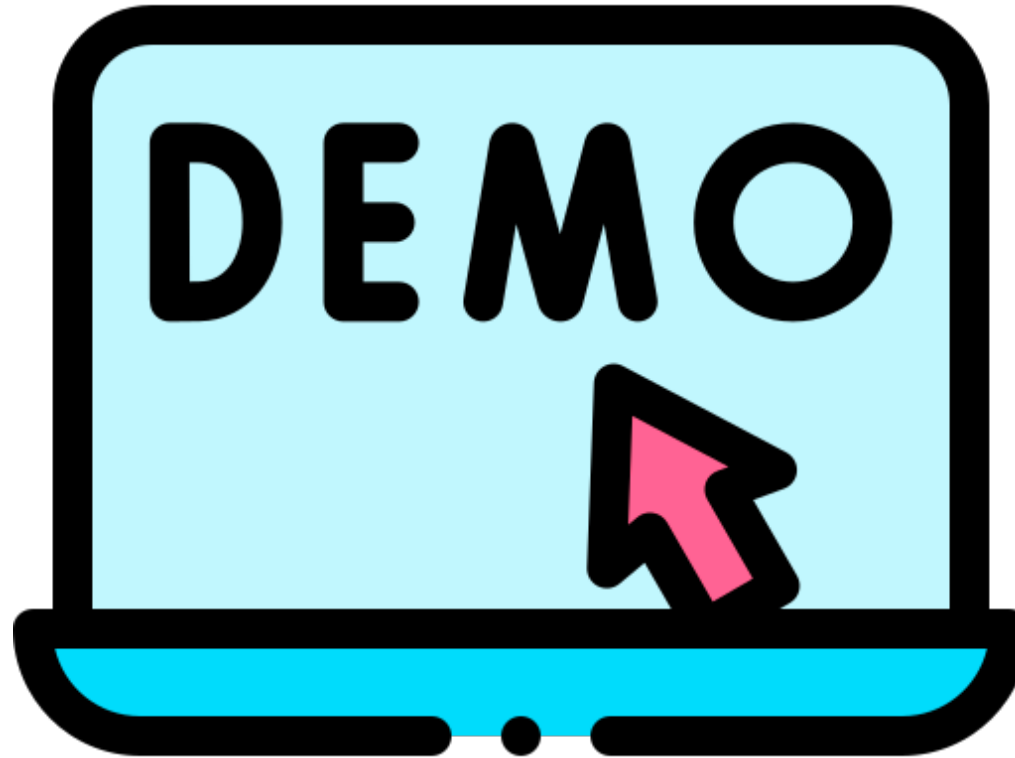
# Basics of Cryptography and Applications

## Cryptographic Hash Functions



## Basics of Cryptography and Applications

# Cryptographic Hash Functions



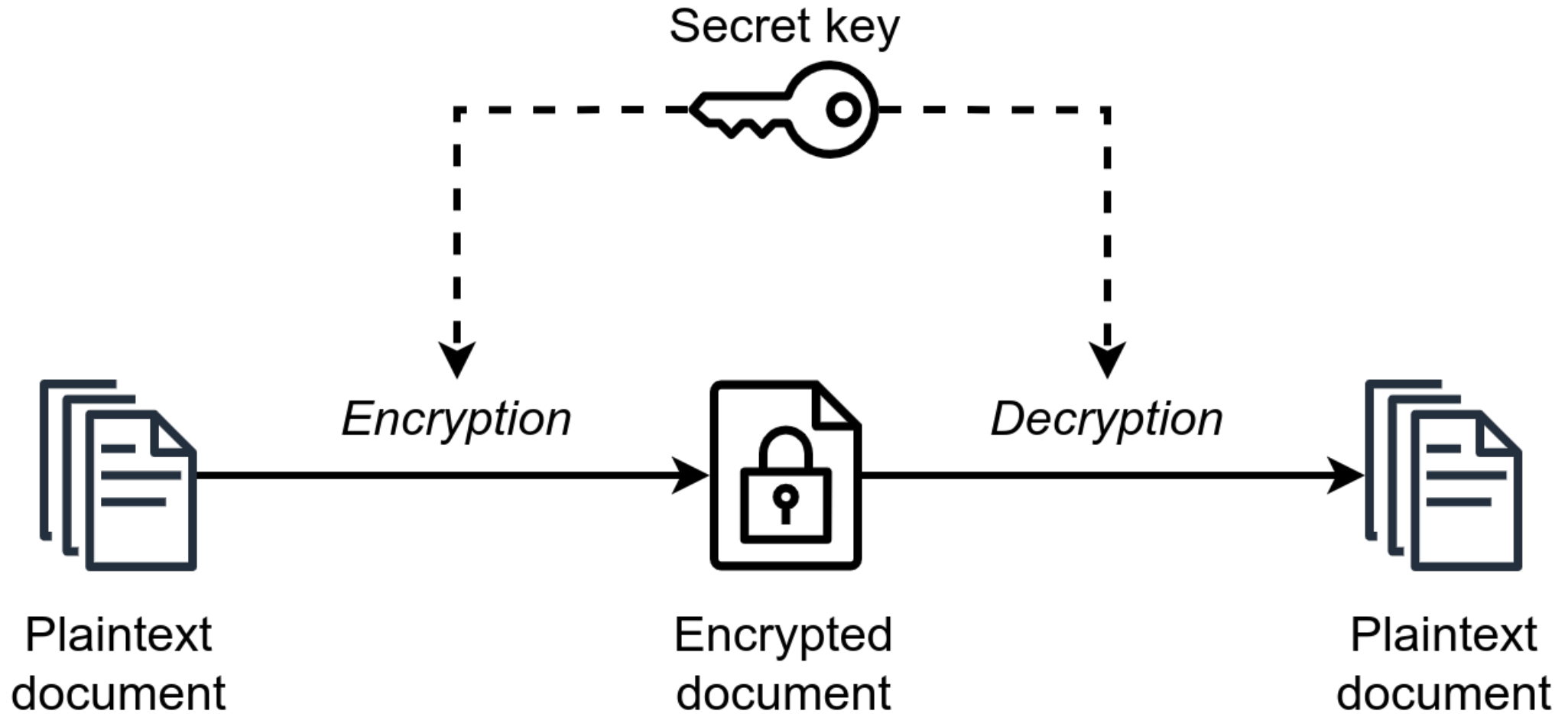
# Agenda

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



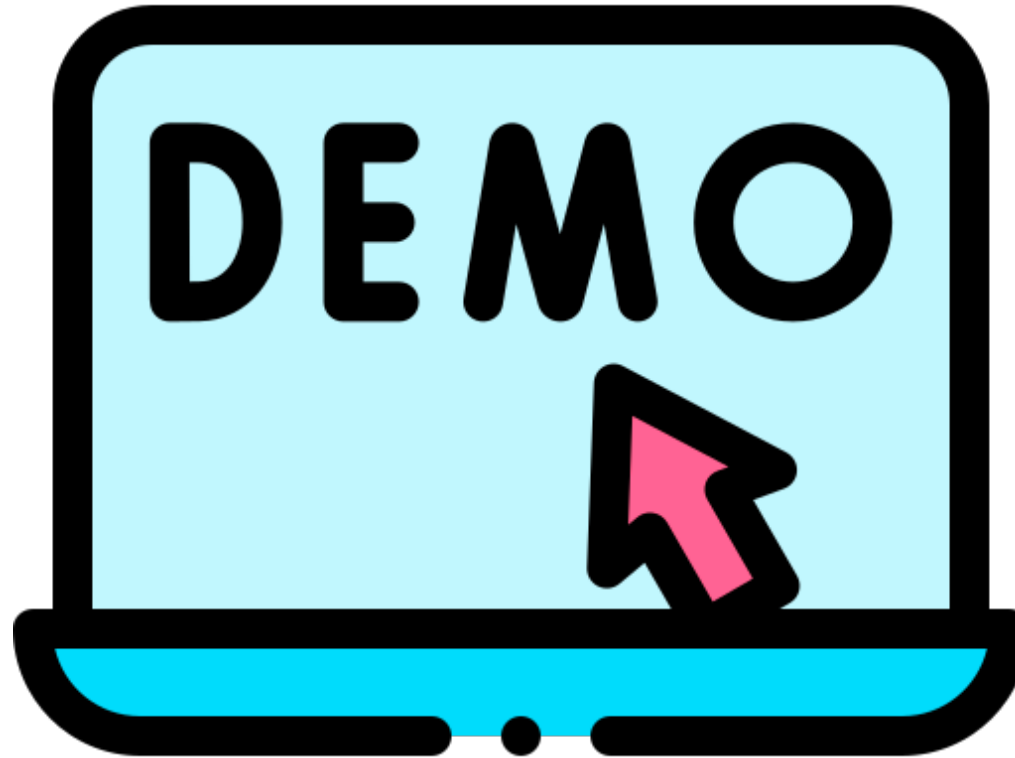
## Basics of Cryptography and Applications

# Symmetric Key Cryptography



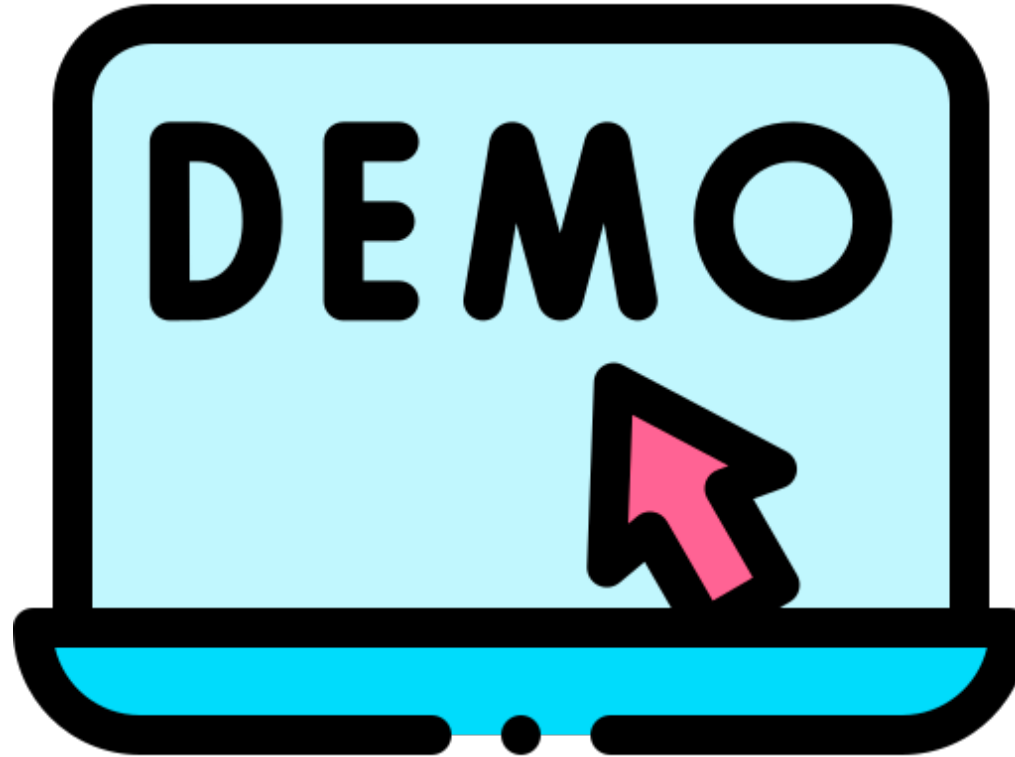
## Basics of Cryptography and Applications

### Demo - DES Encryption/Decryption



## Basics of Cryptography and Applications

### Demo - AES Encryption/Decryption

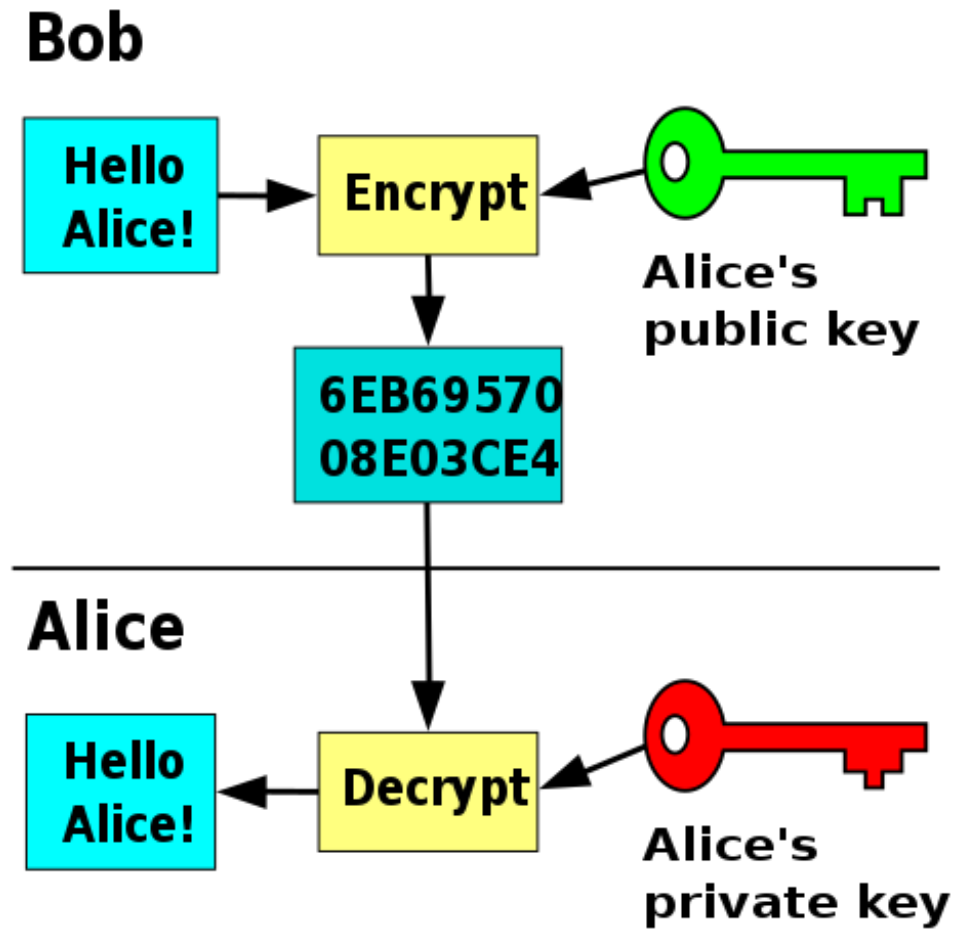


# Agenda

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

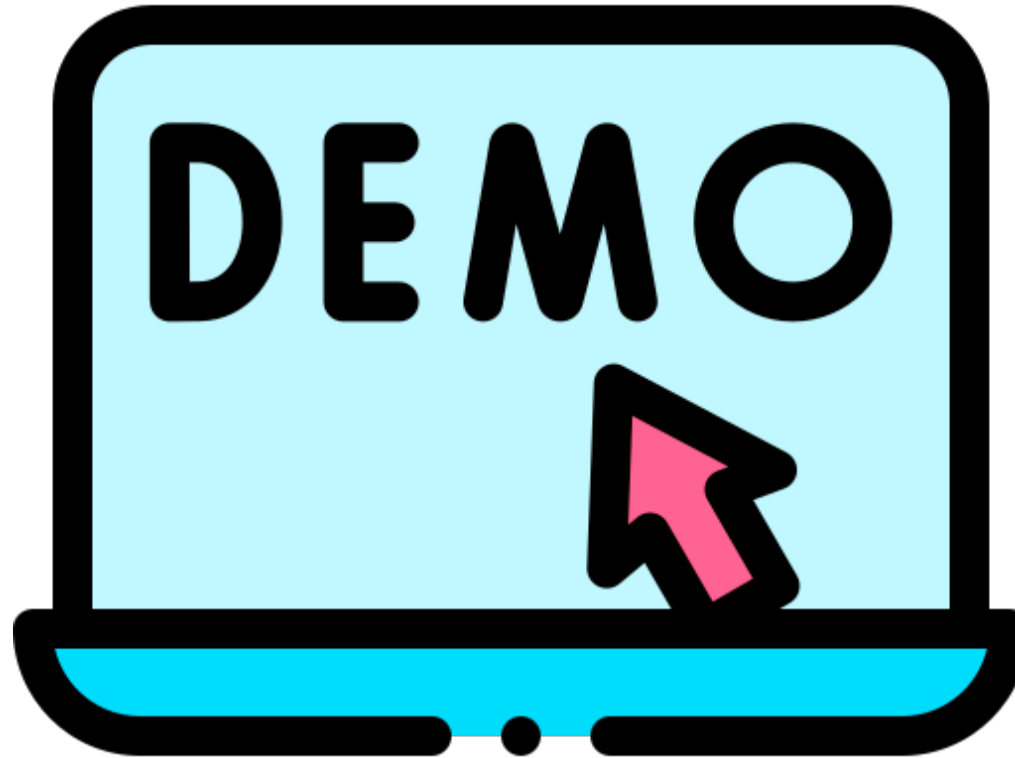
# Basics of Cryptography and Applications

## Asymmetric Key Cryptography



# Basics of Cryptography and Applications

## Demo - RSA Encryption/Decryption

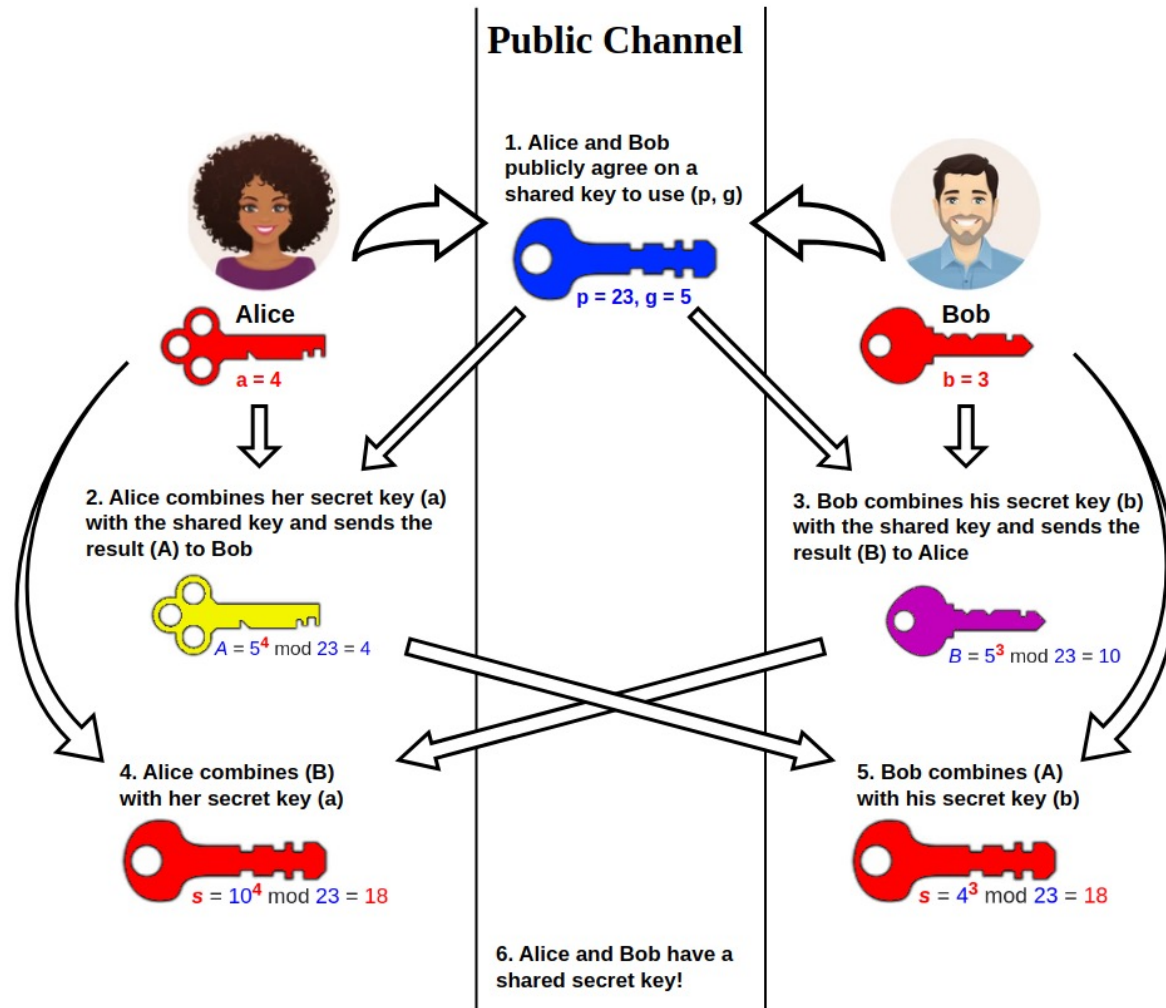


# Agenda

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

# Basics of Cryptography and Applications

## Cryptography Applications - Diffie-Hellman Key Exchange





## Basics of Cryptography and Applications

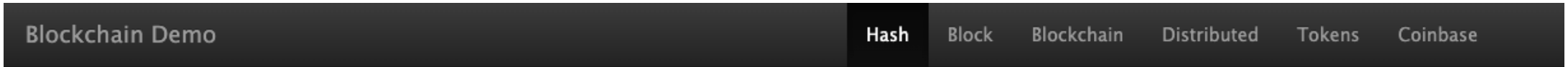
# Cryptography Applications - Git SSH Key

```
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



## SHA256 Hash

A web-based interface for calculating a SHA256 hash. It features a large text input field labeled "Data:" and a corresponding output field labeled "Hash:" containing the hash value "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855". A small green circular logo with a white 'G' is visible in the bottom right corner of the interface.

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

# Basics of Cryptography and Applications

## 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



# Basics of Cryptography and Applications

**THANK YOU FOR LISTENING...**