

CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Symmetric Encryption Applications



Video Summary

- Symmetric Encryption for Data Authentication
- Symmetric Encryption for User Authentication
- Symmetric Encryption for Confidentiality



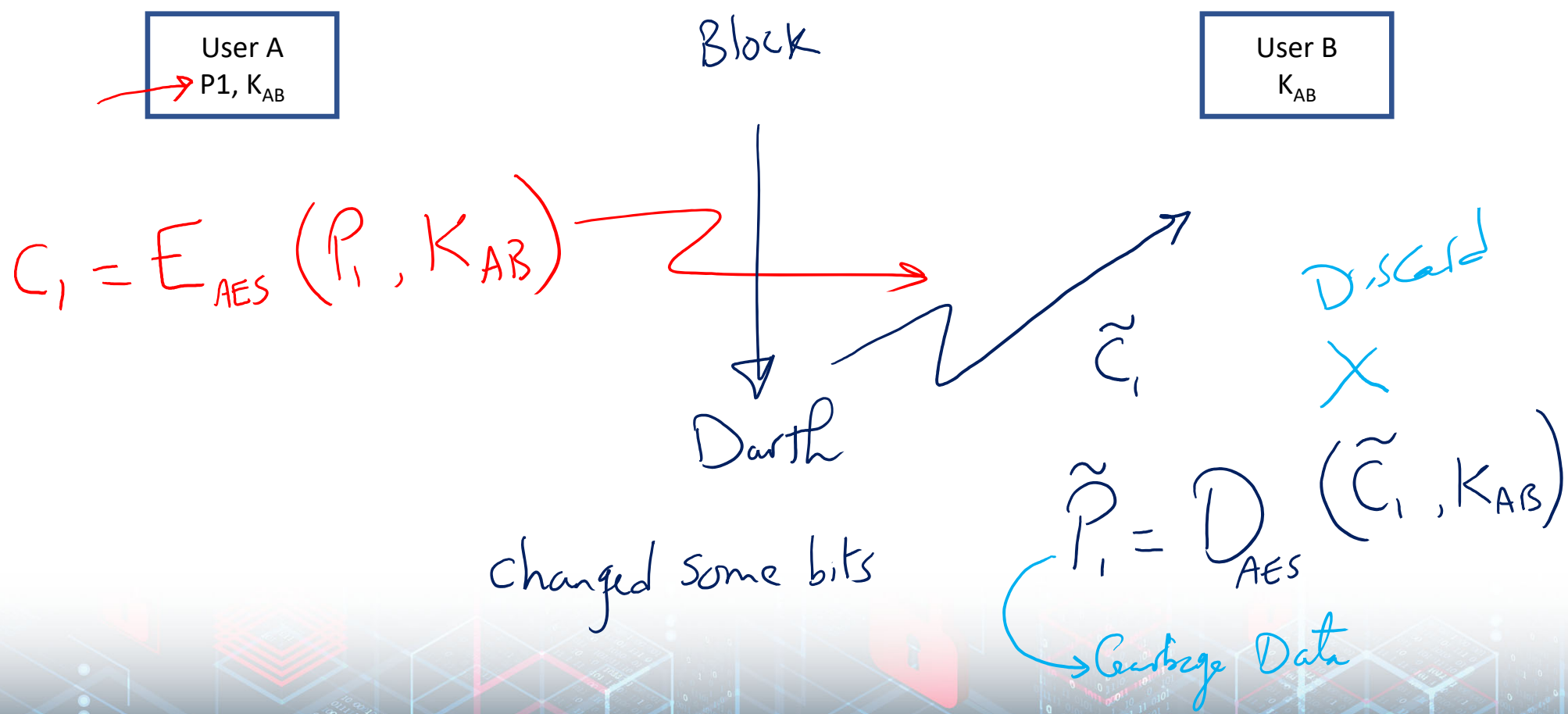
Authentication

- ▶ Receiver wants to verify:
 1. Contents of the message have not been modified (*data authentication*)
 2. Source of message is who they claim to be (*source authentication*)
- ▶ Different approaches available:
 - ▶ Symmetric Key Encryption ✓
 - ▶ Message Authentication Codes
 - ▶ Hash Functions
 - ▶ Public Key Encryption (see Digital Signatures)



Wants to Receive P_1

Symmetric Encryption for Data Authentication



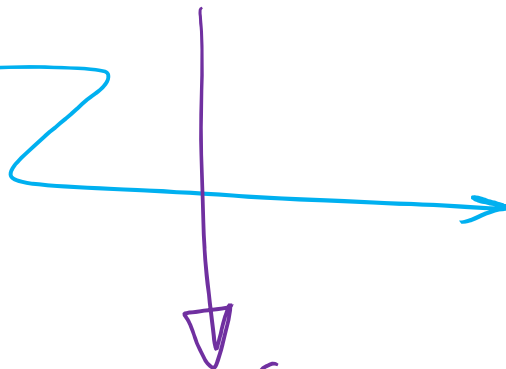
Symmetric Encryption for User Authentication

User A
 P_1, K_{AB}

User B
 K_{AB}

$$C_1 = E_{AES}(P_1, K_{AB})$$

X



Darth

$$C_2 = E_{AES}(P_2, K_{XY})$$

$$P_x = D_{AES}(C_2, K_{AB})$$

Garbage Data

C_2 will be discarded

Symmetric Encryption for Data Confidentiality

User A
 P_1, K_{AB}

User B
 K_{AB}

$$C_1 = E_{AES}(P_1, K_{AB}) \longrightarrow P_1 = D_{AES}(C_1, K_{AB})$$

↓
Darth
Try to Decrypt
using $K_{X,Y}$ (Different Key)

Video Summary

- Symmetric Encryption for Data Authentication ✓
- Symmetric Encryption for User Authentication ✓
- Symmetric Encryption for Confidentiality ✓

