CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Symmetric Encryption Applications

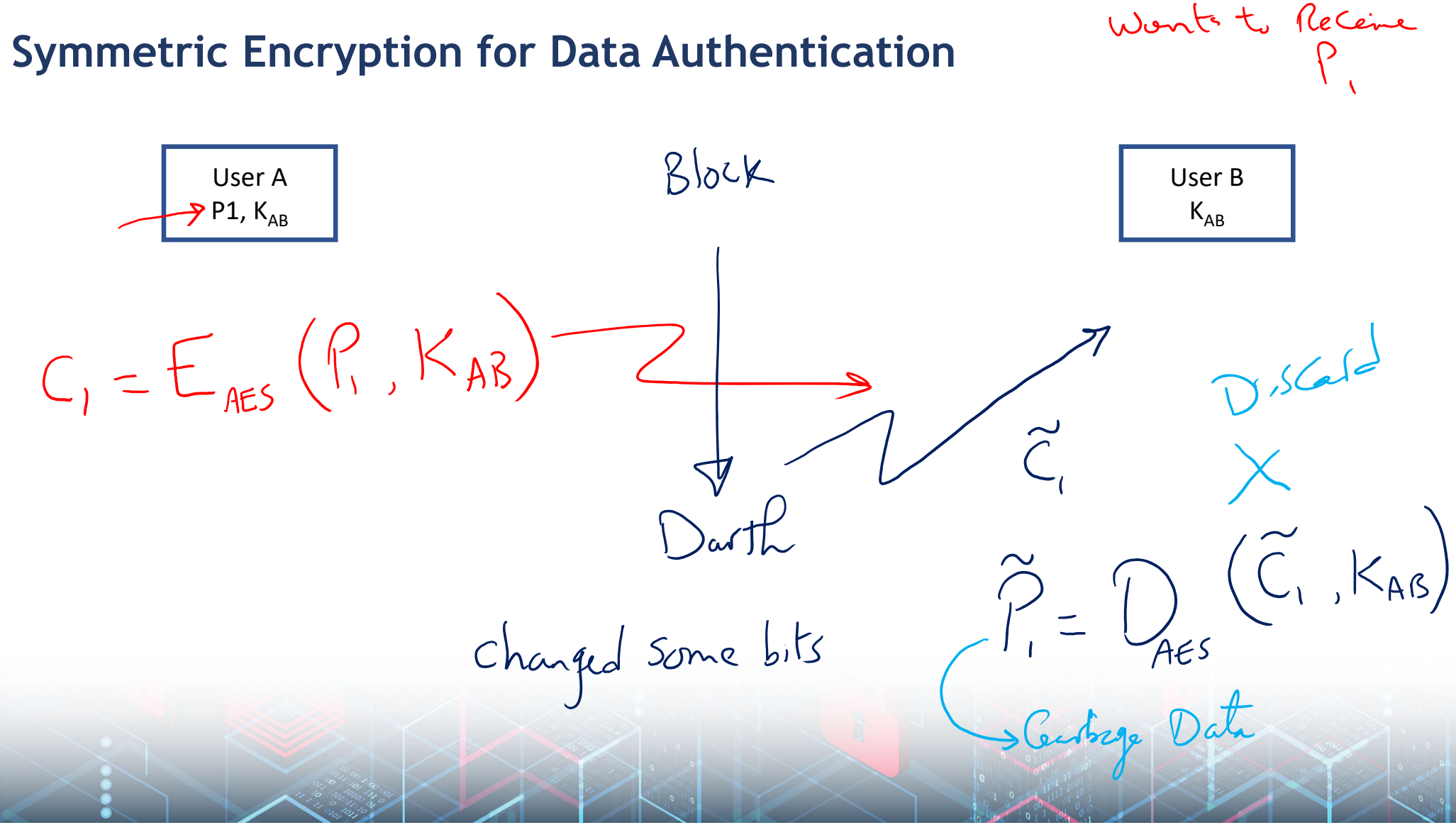
Video Summary

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

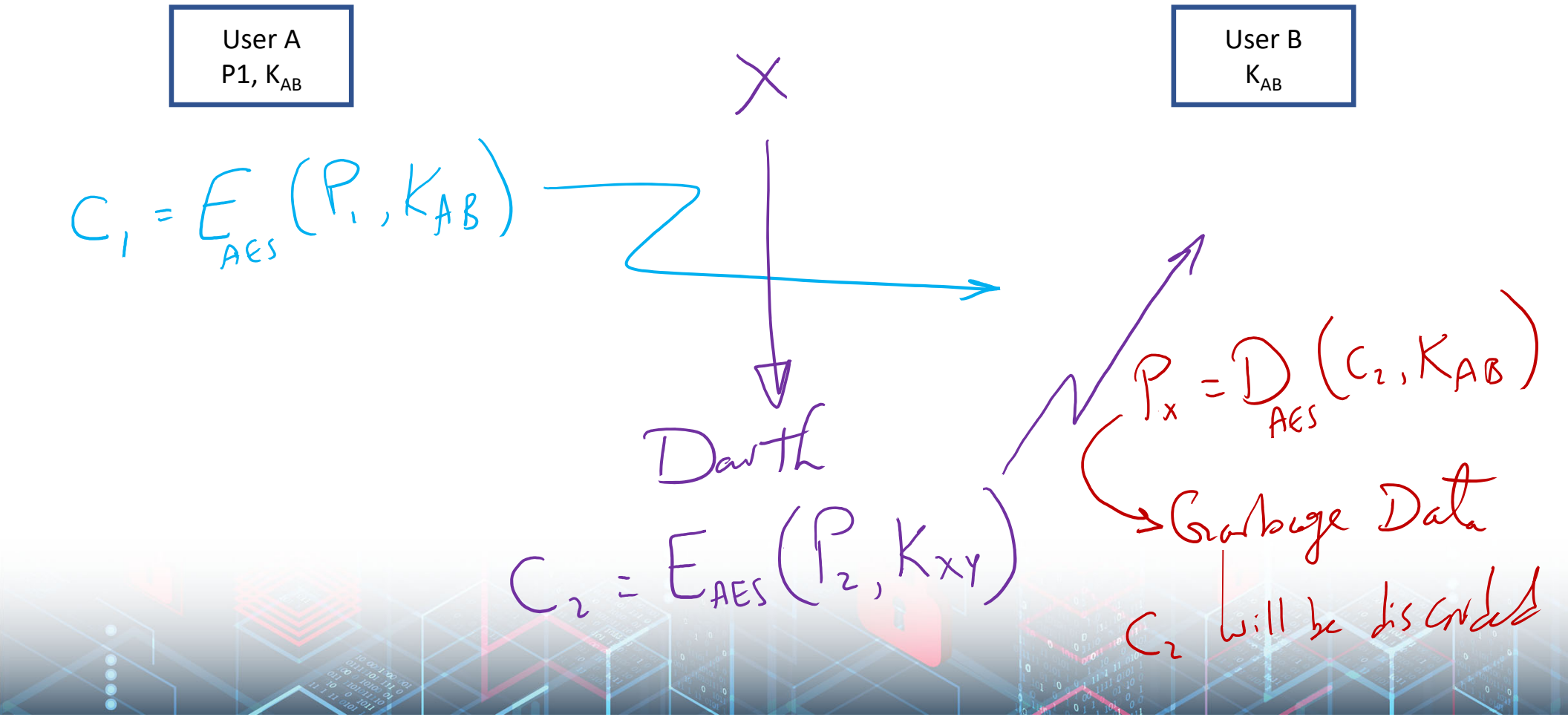
Authentication

- 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)

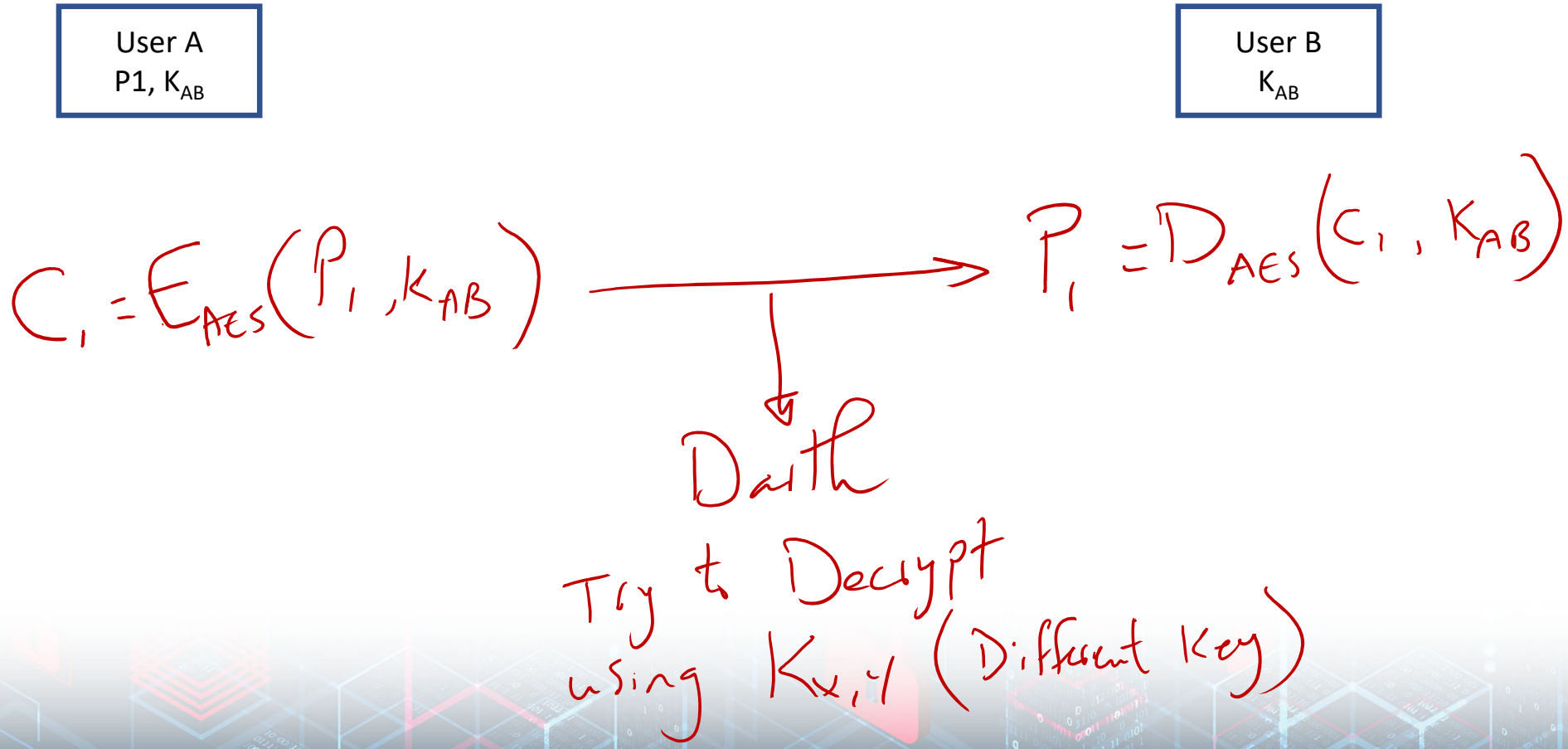
Symmetric Encryption for Data Authentication



Symmetric Encryption for User Authentication



Symmetric Encryption for Data Confidentiality



Video Summary

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