

# Introduction to Modern Cryptography



8th lecture:

Private-Key Management and the  
Public-Key Revolution

# Outline of the Course

	secret key	public key
confidentiality	private-key encryption	public-key encryption
authentication	message authentication codes (MAC)	digital signatures

# Outline of the Course

- reduction proofs
- pseudorandomness
- block ciphers: DES, AES

	secret key	public key
confidentiality	private-key encryption	public-key encryption
authentication	message authentication codes (MAC)	digital signatures

# Outline of the Course

- reduction proofs
- pseudorandomness
- block ciphers: DES, AES

	secret key	public key
confidentiality	private-key encryption	public-key encryption
authentication	message authentication codes (MAC)	digital signatures

- collision-resistant hash functions

# Outline of the Course

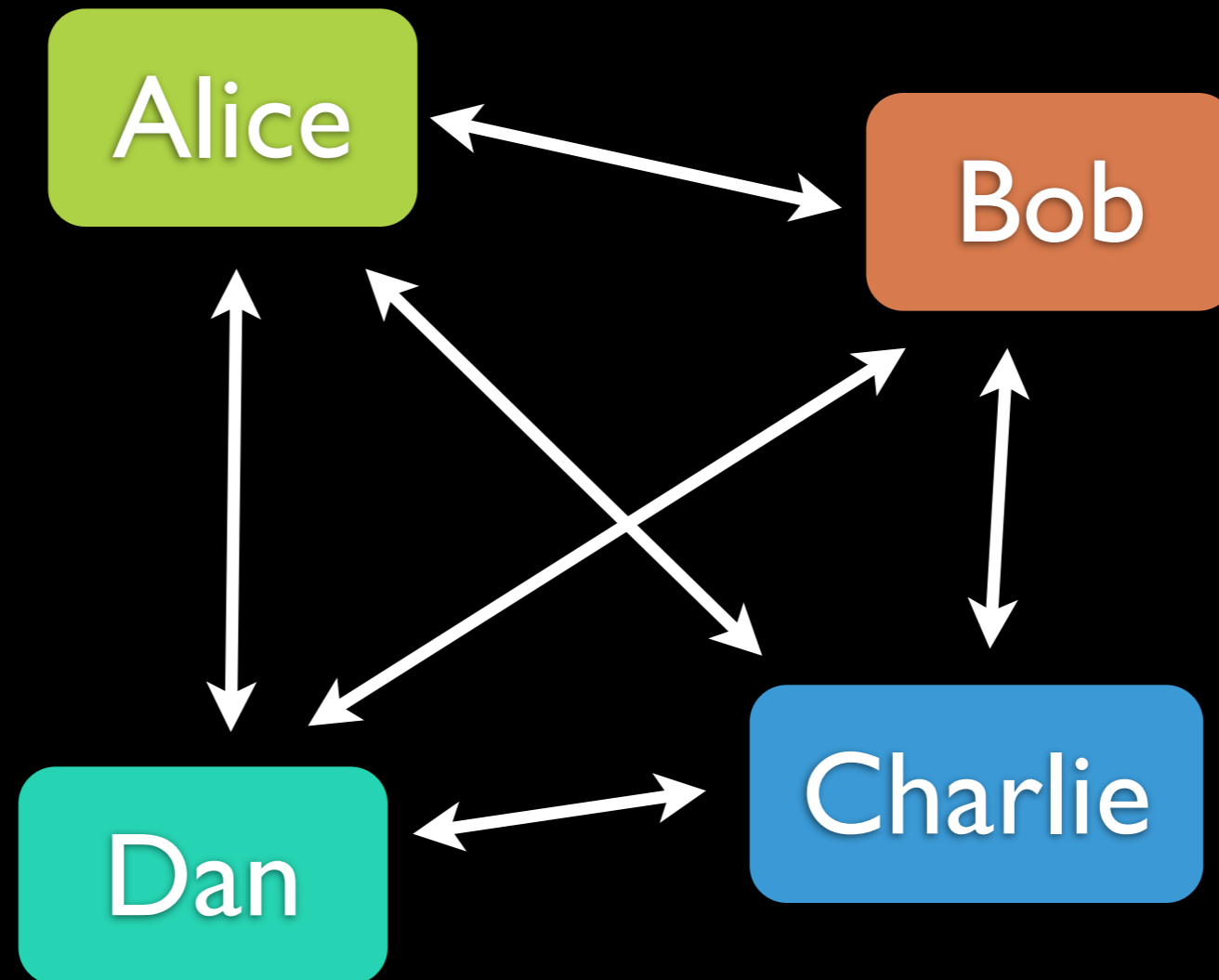
- algorithmic number theory
- key distribution, Diffie-Hellmann
- RSA

- reduction proofs
- pseudorandomness
- block ciphers: DES, AES

	secret key	public key
confidentiality	private-key encryption	public-key encryption
authentication	message authentication codes (MAC)	digital signatures

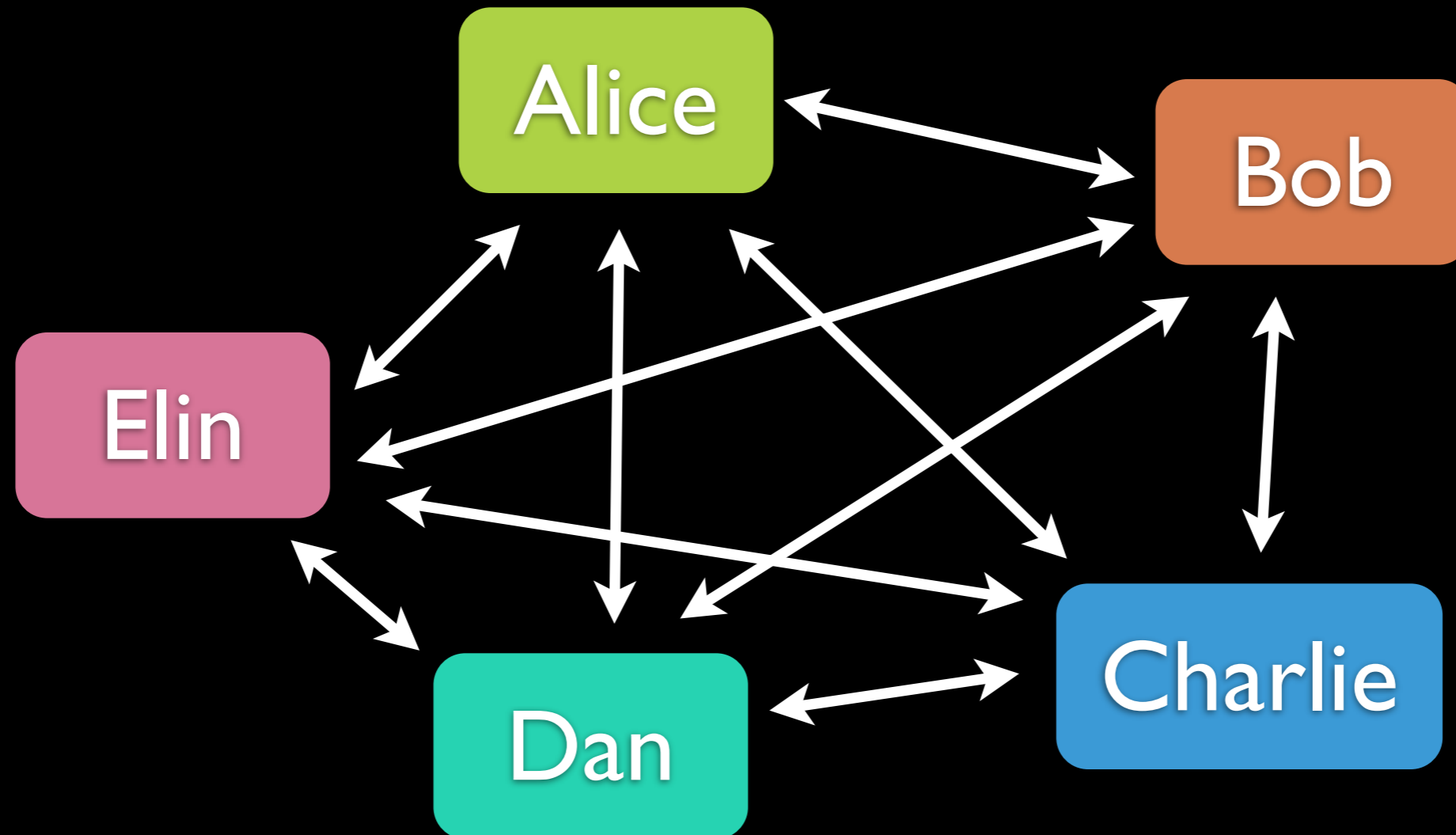
- collision-resistant hash functions

# Key Management: Pairwise Keys



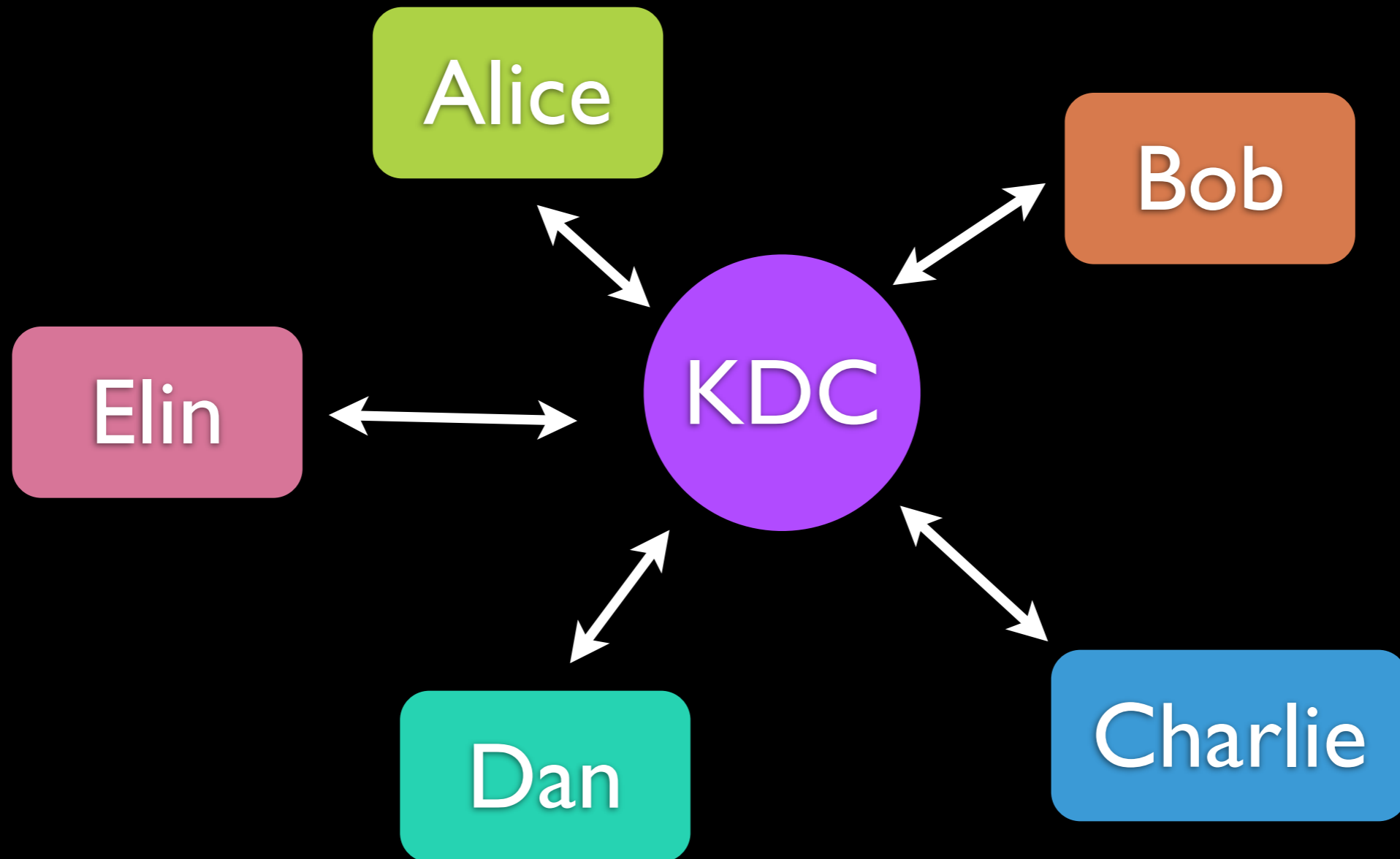
- each of the  $N$  users needs to store  $N-1$  keys
- updating is annoying
- open systems are impossible

# Key Management: Pairwise Keys



- each of the  $N$  users needs to store  $N-1$  keys
- updating is annoying
- open systems are impossible

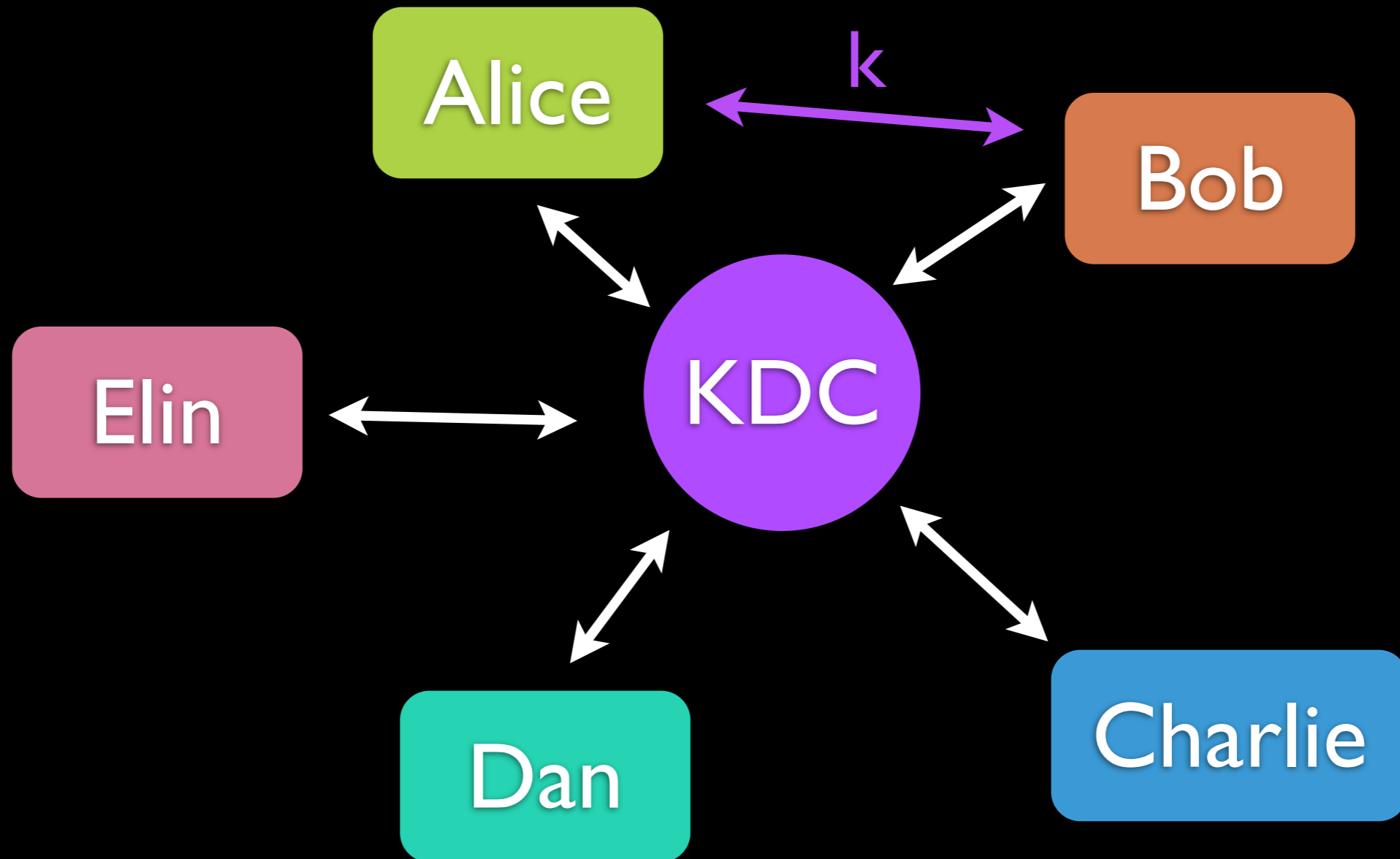
# Key Distribution Center (KDC)



- $\text{Mac}_{k_A}$  (“I want to talk to Bob”)
- session key  $k \leftarrow \text{KDC}$ ,  
sends  $\text{EncMac}_{k_A}(k)$  to Alice and  $\text{EncMac}_{k_B}(k)$  to Bob
- or sends  $\text{EncMac}_{k_A}(k, \text{EncMac}_{k_B}(k))$  to Alice

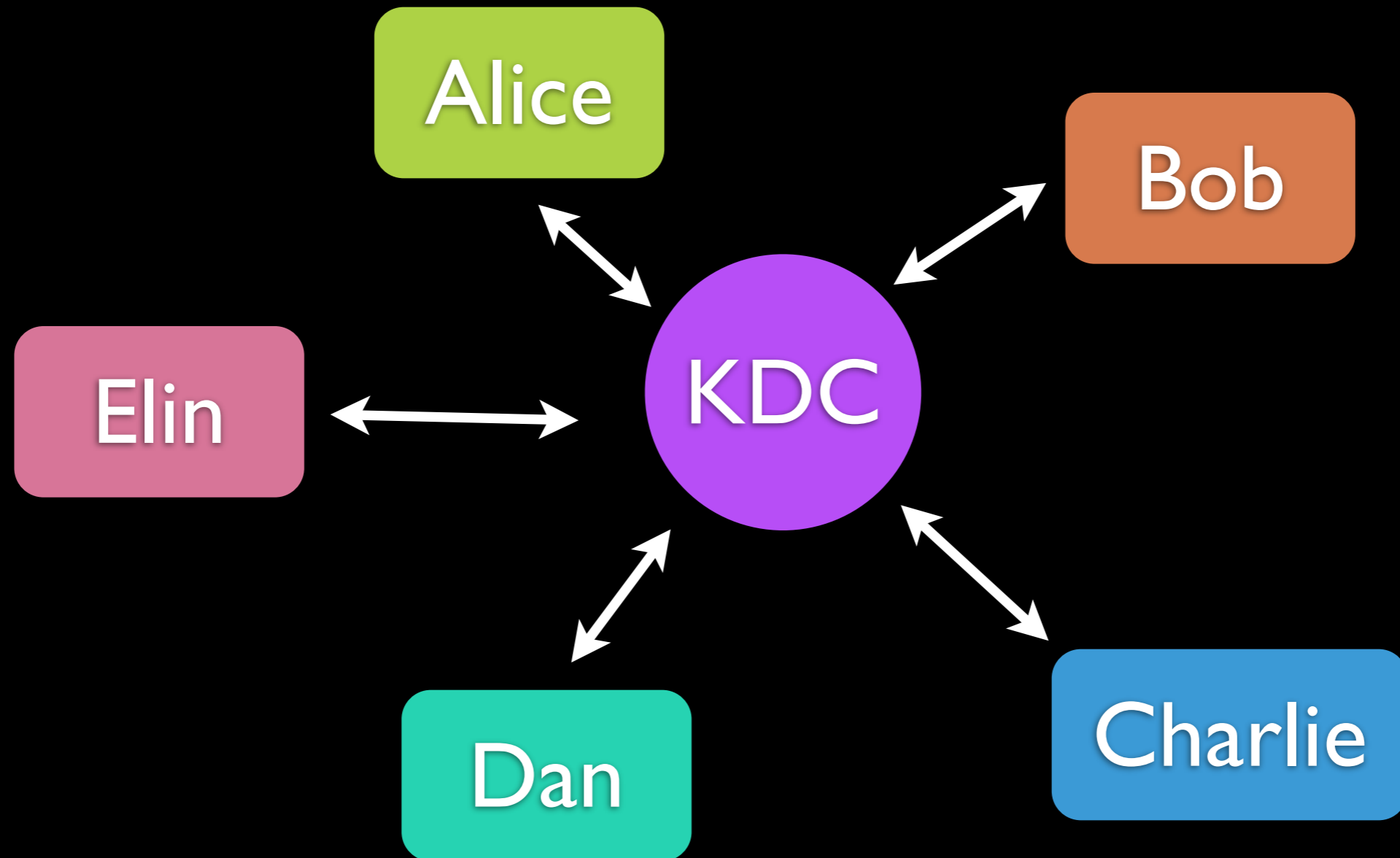


# Key Distribution Center (KDC)



- $\text{Mac}_{k_A}$  (“I want to talk to Bob”)
- session key  $k \leftarrow \text{KDC}$ ,  
sends  $\text{EncMac}_{k_A}(k)$  to Alice and  $\text{EncMac}_{k_B}(k)$  to Bob
- or sends  $\text{EncMac}_{k_A}(k, \text{EncMac}_{k_B}(k))$  to Alice

# Key Distribution Center (KDC)



- users have to store only one key
- update only one key
- **single point of failure / single point of attack**

# Whitfield Diffie

\*1944



- BSc from MIT
- honorary PhD from ETH Zurich
- working at Sun

# Martin Edward Hellman

\*1945



- IBM Watson
- MIT, Stanford
- [NuclearRisk.org](http://NuclearRisk.org)