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

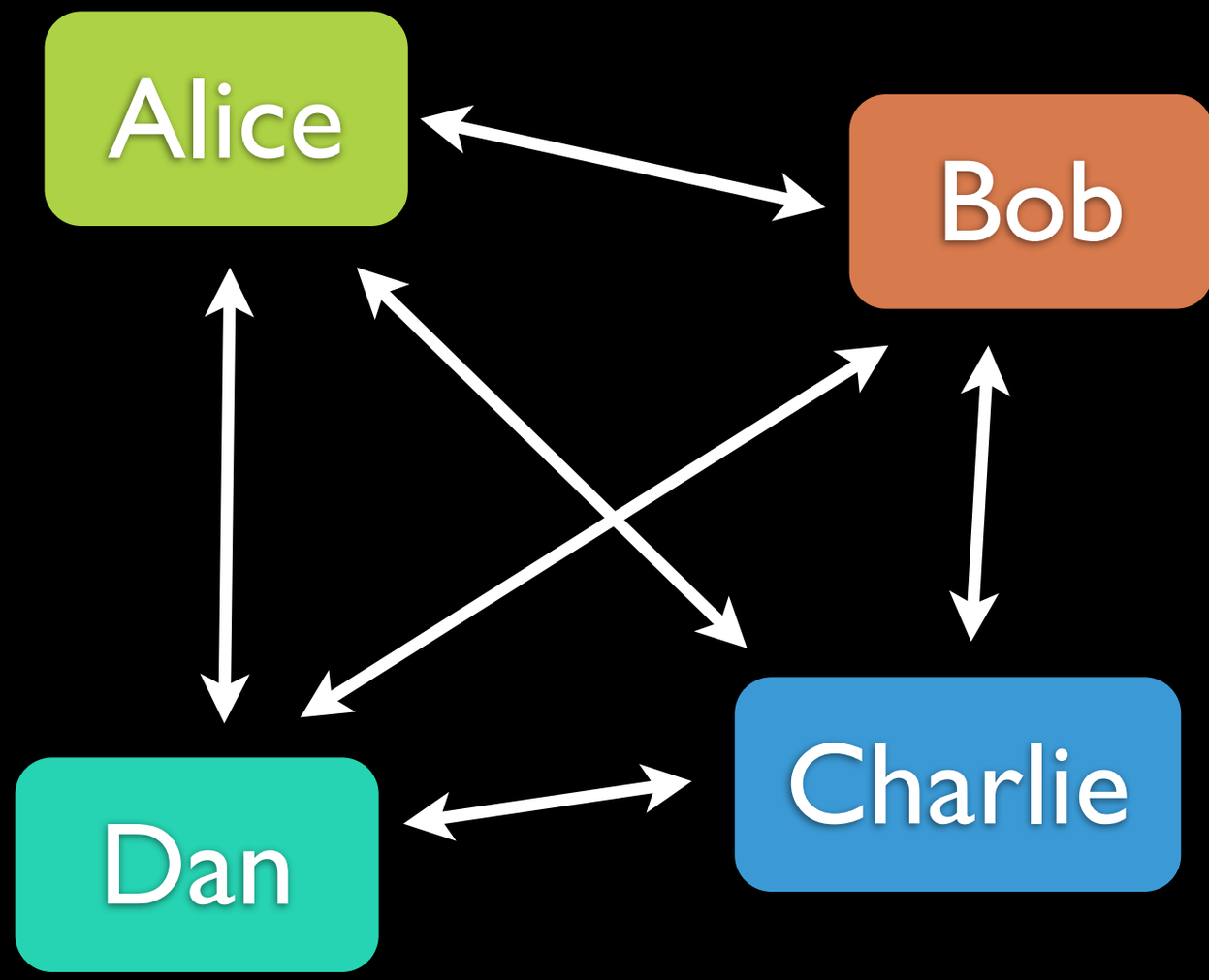
- algorithmic number theory
- key distribution, Diffie-Hellmann
- RSA

- 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

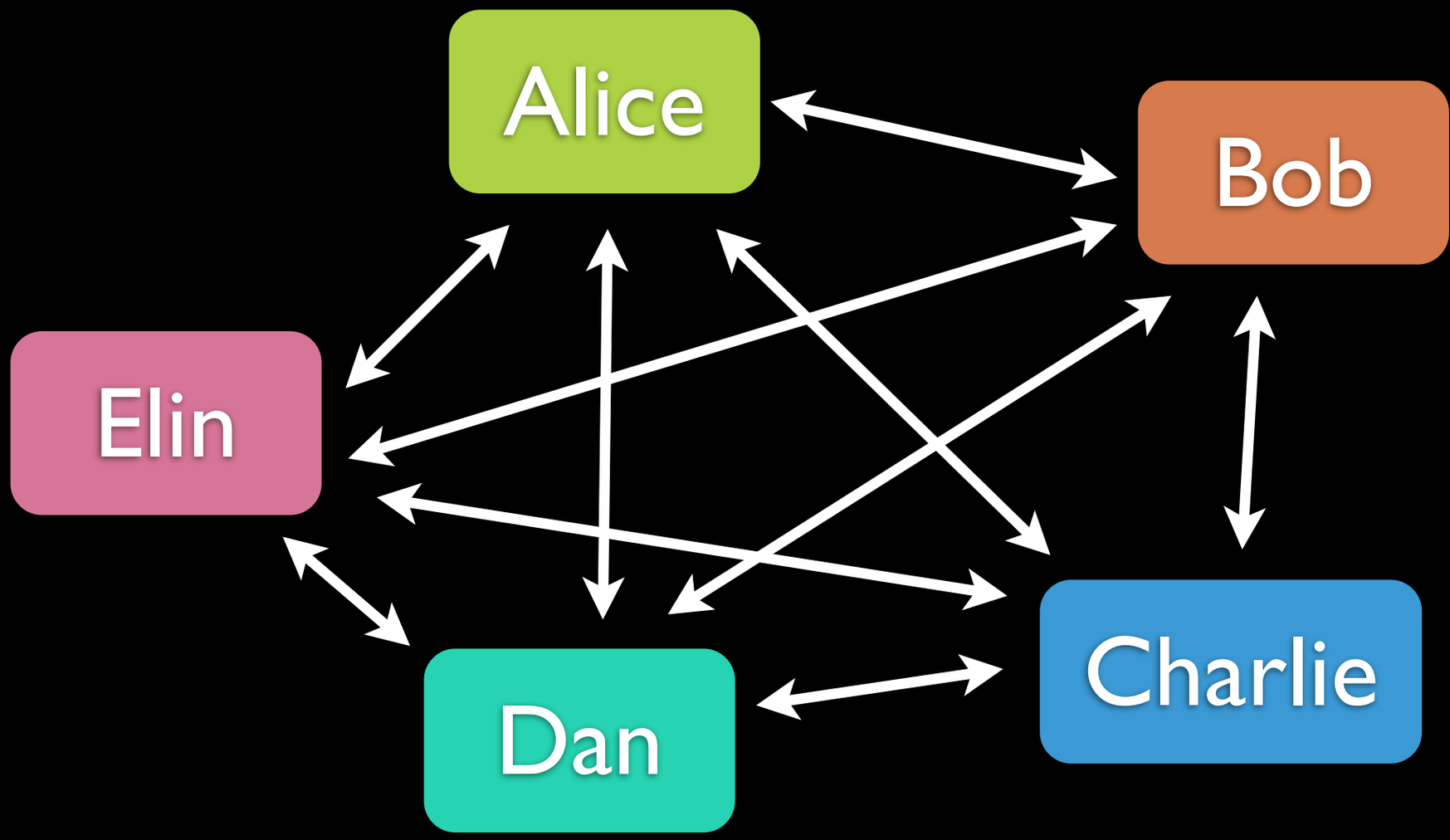
- collision-resistant hash functions

Key Management: Pairwise Keys



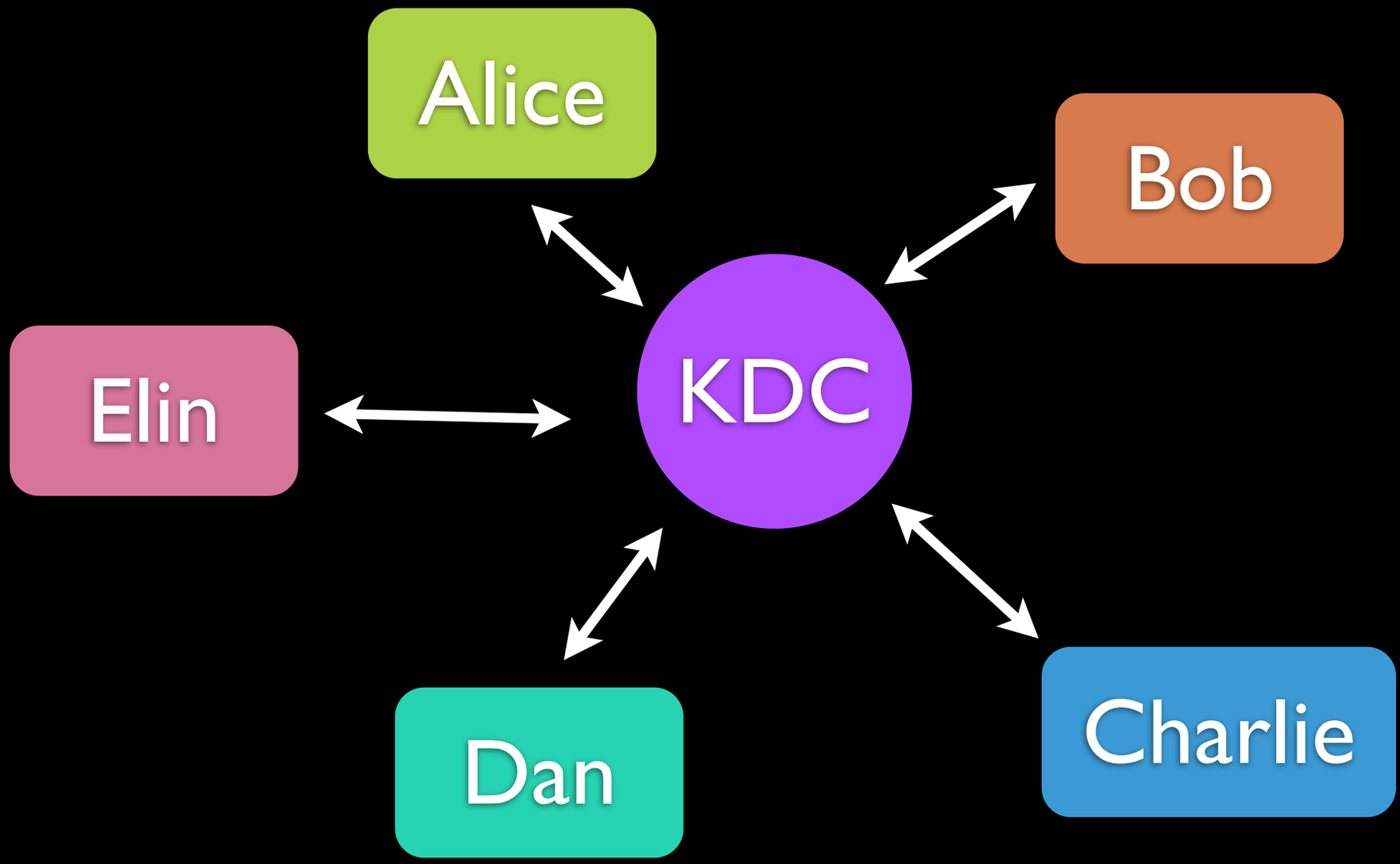
- each of the N users needs to store N-1 keys
- updating is annoying
- open systems are impossible

Key Management: Pairwise Keys



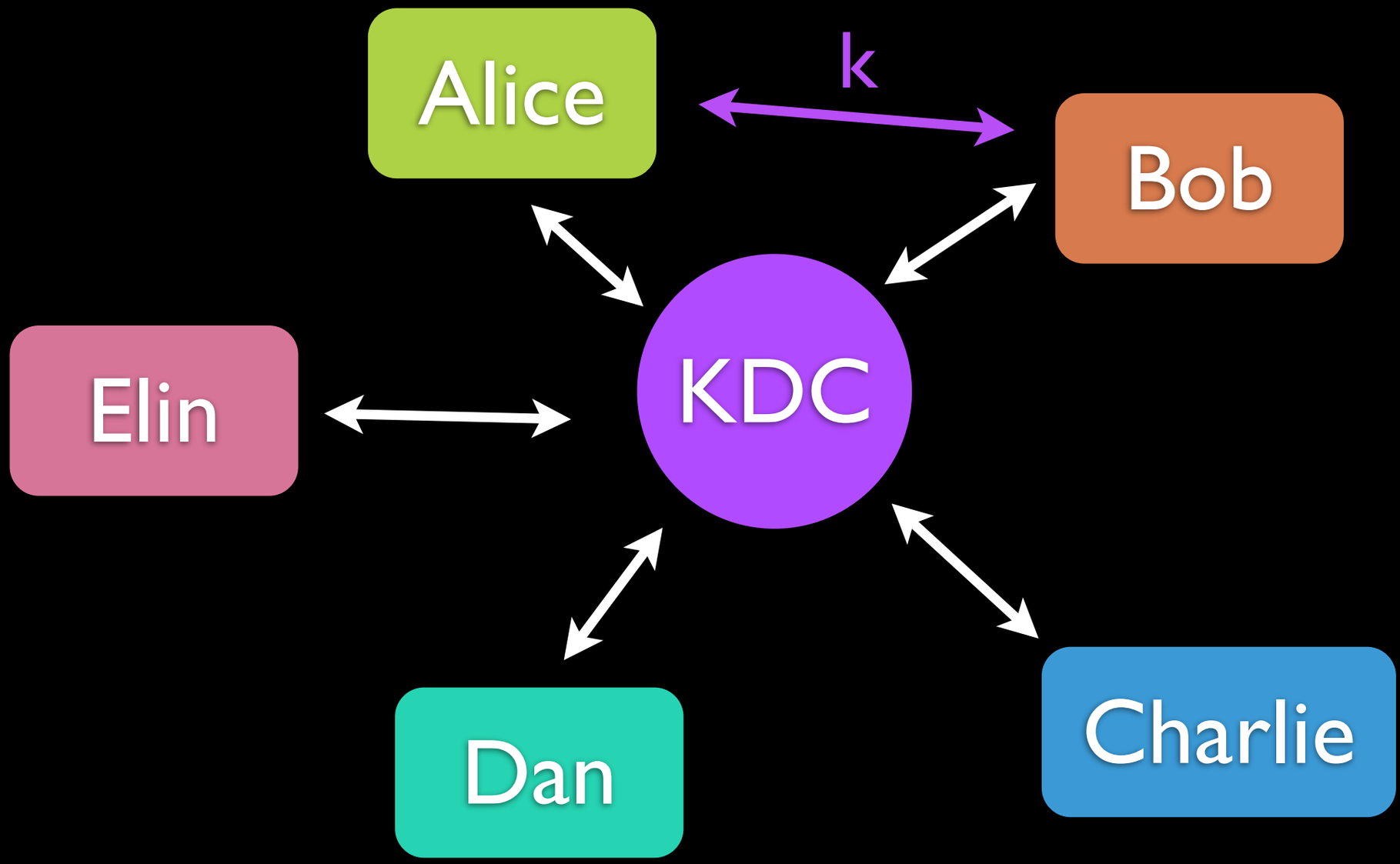
- each of the N users needs to store N-1 keys
- updating is annoying
- open systems are impossible

Key Distribution Center (KDC)



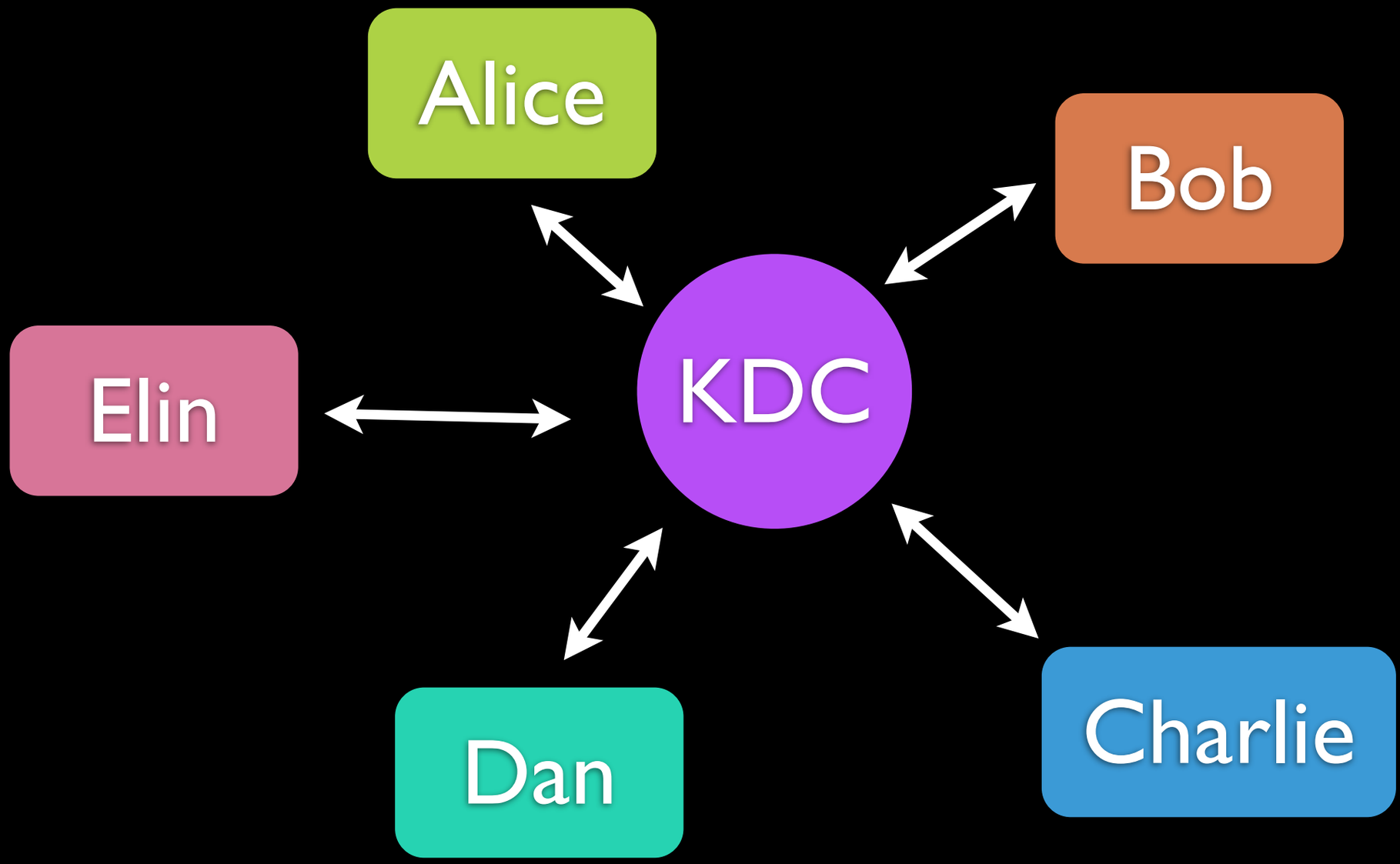
- Mac_{kA}(“I want to talk to Bob”)
- session key $k \leftarrow$ KDC,
  sends $EncMac_{kA}(k)$ to Alice and $EncMac_{kB}(k)$ to Bob
- or sends $EncMac_{kA}(k, EncMac_{kB}(k))$ to Alice

Key Distribution Center (KDC)



- Mac_{kA}(“I want to talk to Bob”)
- session key k←KDC,
  sends $EncMac_{kA}$(k) to Alice and $EncMac_{kB}$(k) to Bob
- or sends $EncMac_{kA}$(k, $EncMac_{kB}$(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