Introduction to Modern Cryptography

8th lecture:

Private-Key Management and the Public-Key Revolution last time:

- practical block ciphers: AES & DES

8th lecture (today):

- Private-Key Management
- Public-Key Revolution

- 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

last time:

- practical block ciphers: AES & DES

8th lecture (today):

- Private-Key Management
- Public-Key Revolution

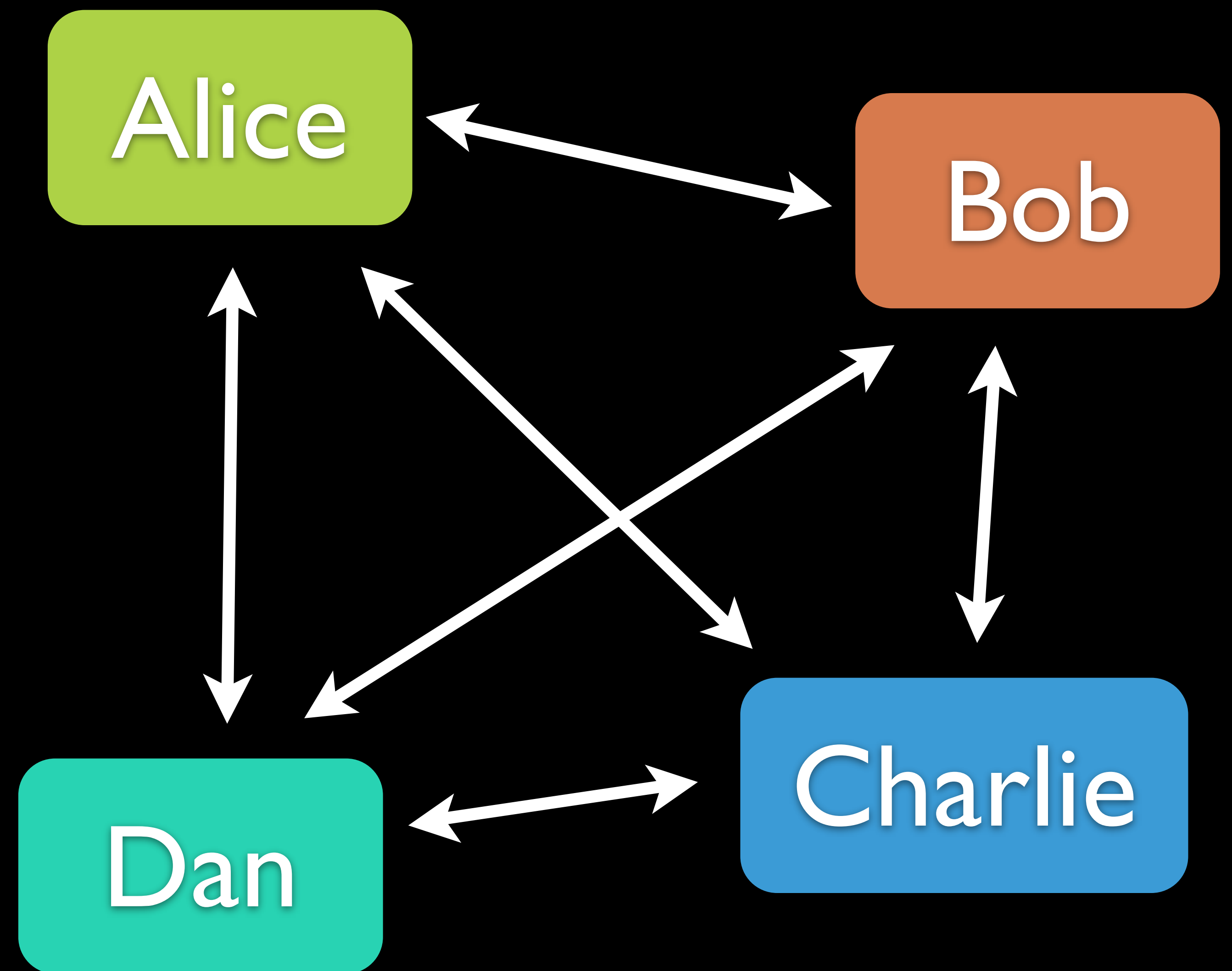
- algorithmic number theory
- key distribution, Diffie-Hellmann
- RSA

- 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

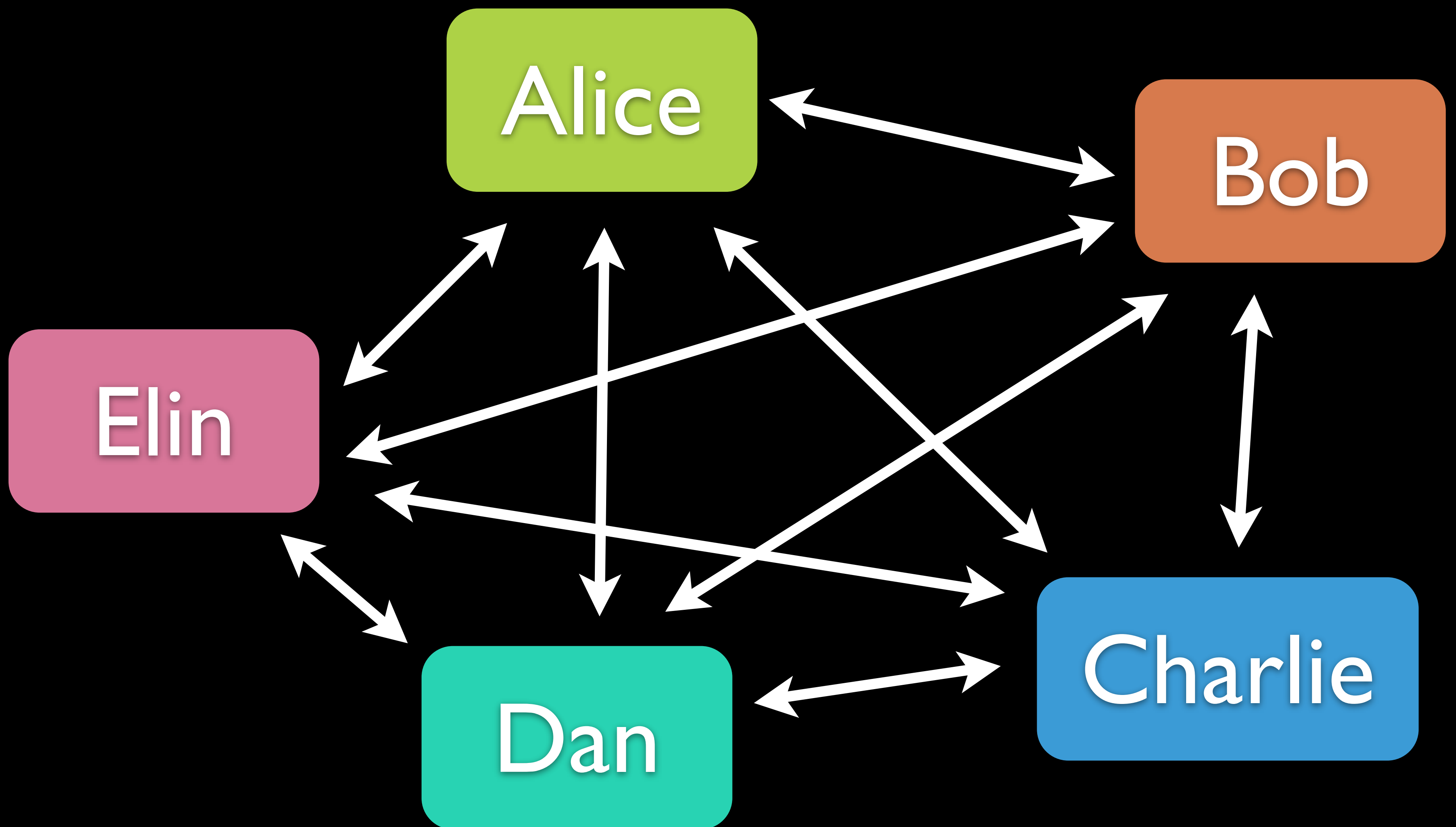
- collision-resistant hash functions

Key Management: Pairwise Keys



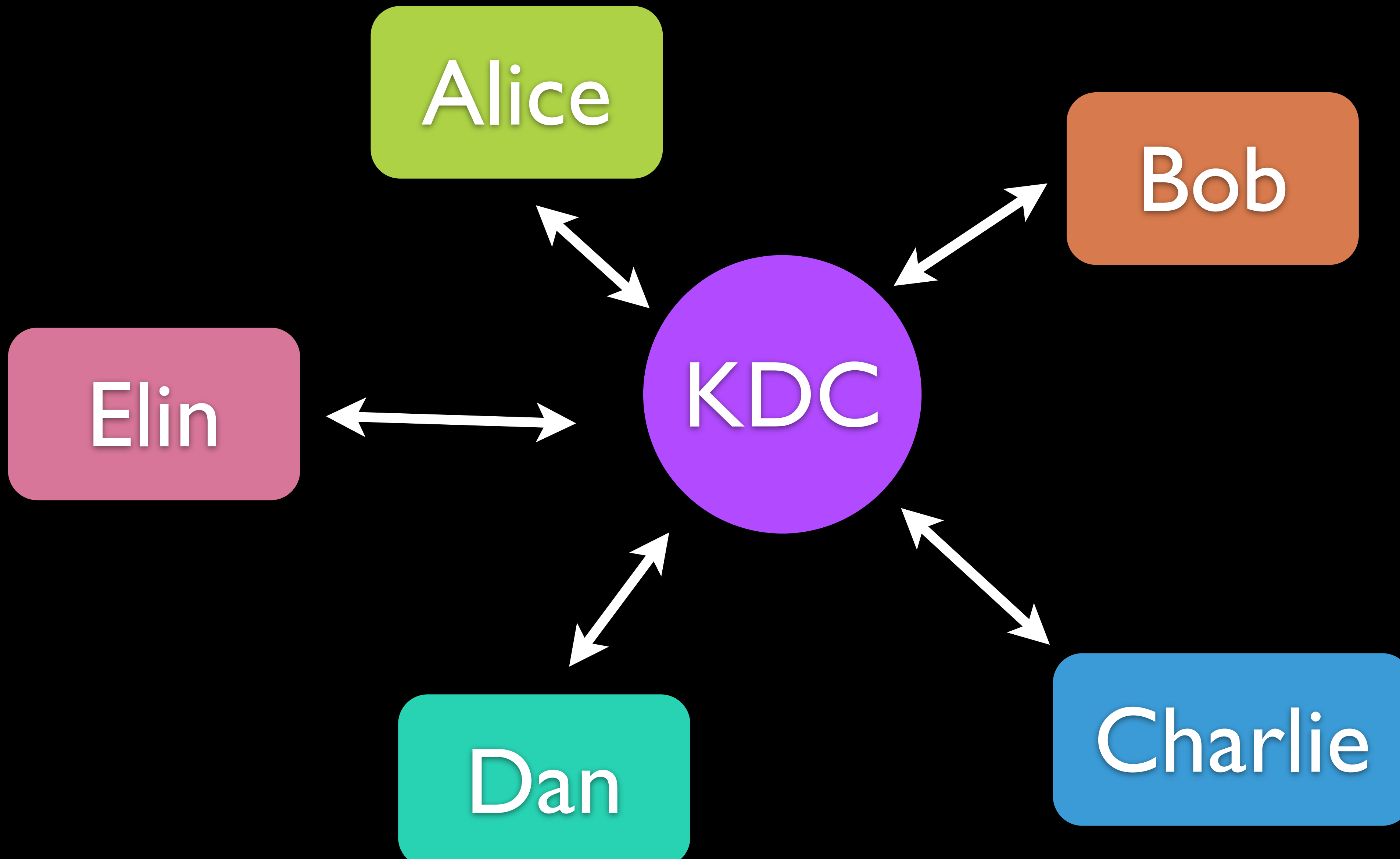
- each of the N users needs to store N-1 keys
- updating is annoying
- open systems are impossible

Key Management: Pairwise Keys



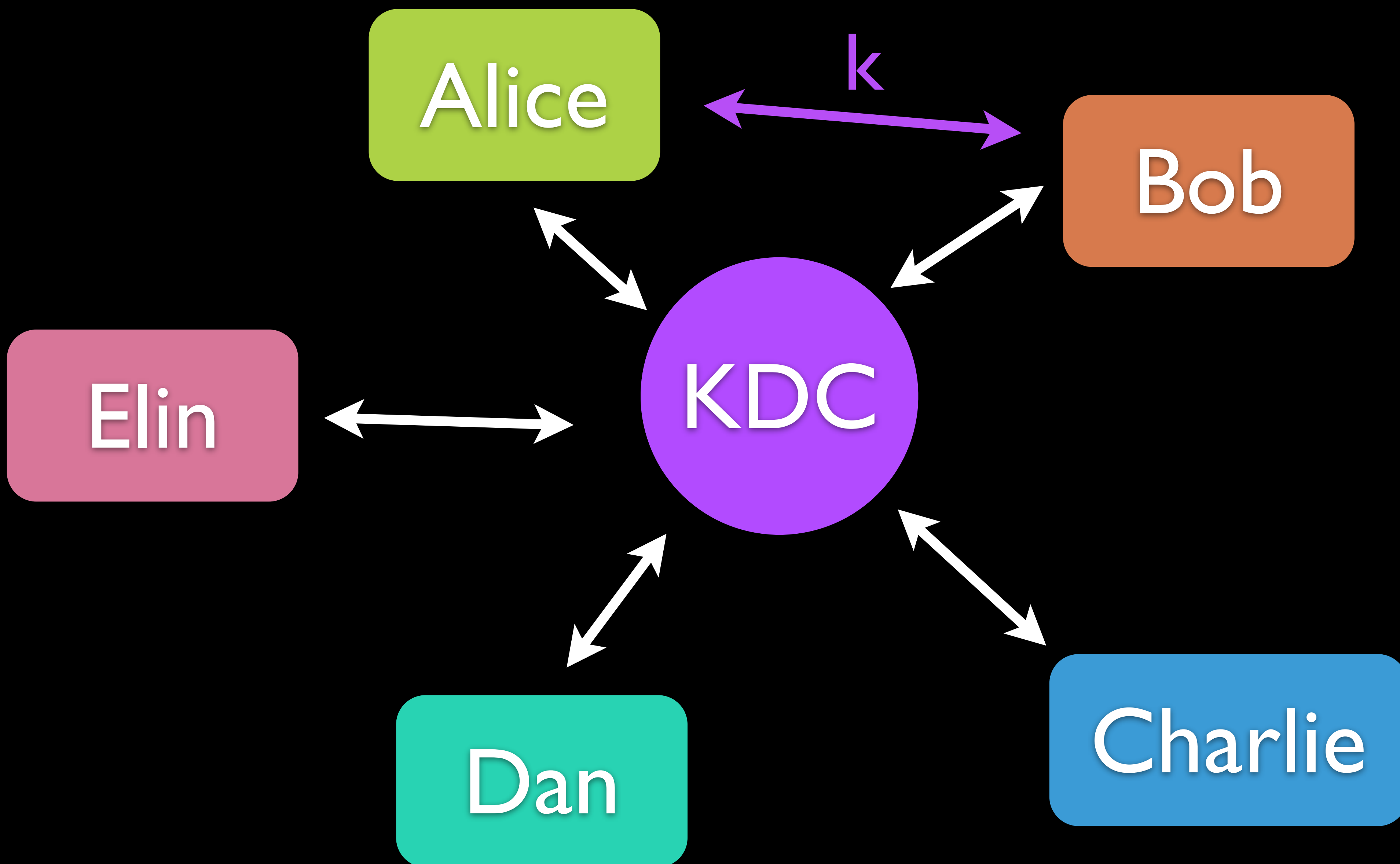
- each of the N users needs to store N-1 keys
- updating is annoying
- open systems are impossible

Key Distribution Center (KDC)



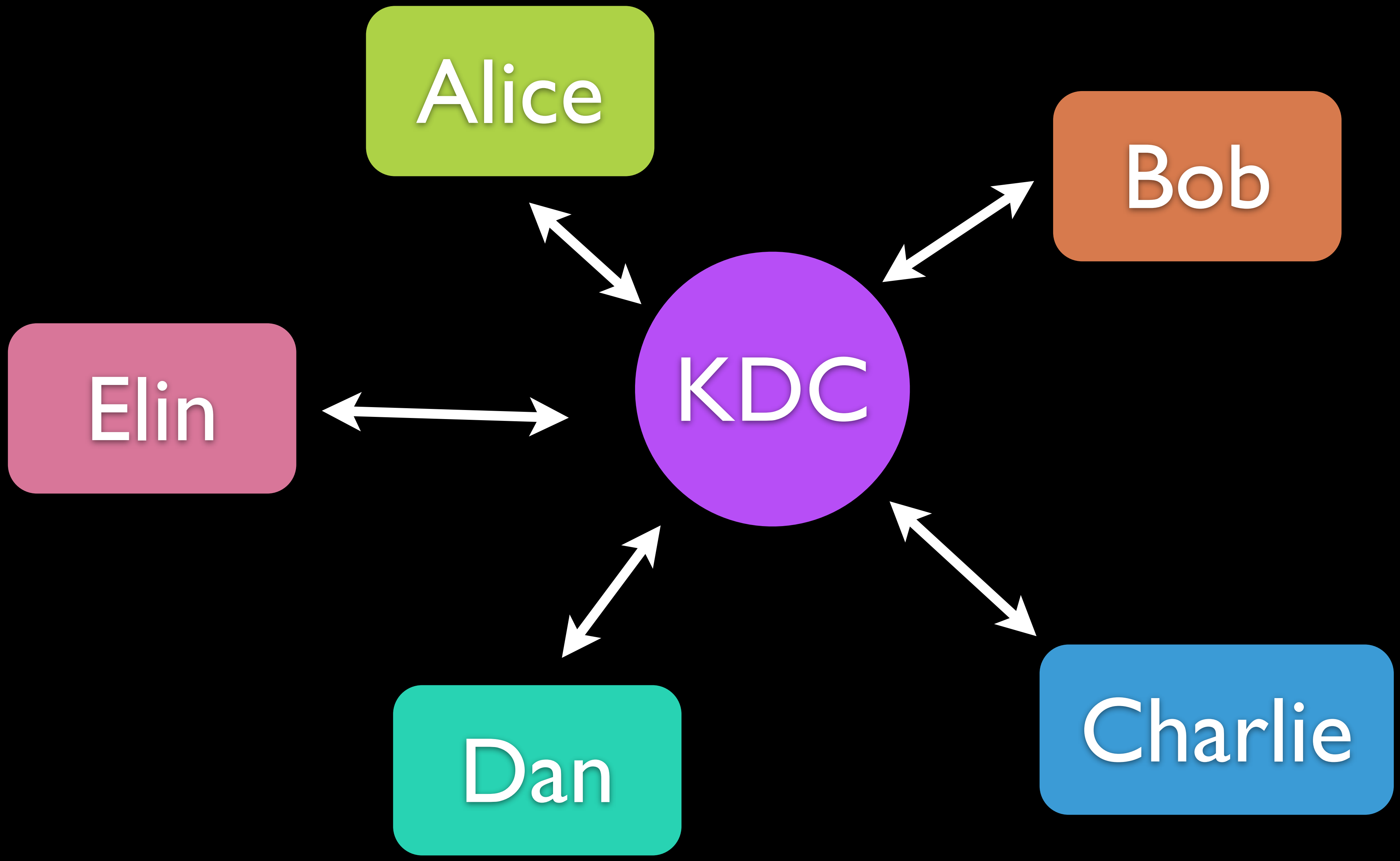
- Mac_{kA}("I want to talk to Bob")
- session key $k \leftarrow$ KDC,
  sends $\mathrm{EncMac}_{kA}(k)$ to Alice and $\mathrm{EncMac}_{kB}(k)$ to Bob
- or sends $\mathrm{EncMac}_{kA}(k, \mathrm{EncMac}_{kB}(k))$ to Alice

Key Distribution Center (KDC)



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

Group Isomorphism

Def: For two groups $(H,\bullet)$ and (G, x), $f{:}H \rightarrow G$ is a group isomorphism from H to G if

$$H \cong G$$

1. f is bijective
2. for all h_1,h_2 in H: $f(h_1 \times h_2) = f(h_1) \bullet f(h_2)$

F^{-1} might not be efficiently computable!

$(\mathbb{Z}_q, +) \cong (G, \times)$ holds for all cyclic groups G=<g> of order q, but computing the inverse is the discrete-logarithm problem.

Quadratic Residues

Def: y in $\mathbb{Z}_p^*$ is a quadratic residue (QR) if there exists x in $\mathbb{Z}_p^*$ such that $x^2 = y \pmod{p}$

Def: The Jacobi / Legendre symbol is defined as

$$\left(\frac{y}{p}\right) := \begin{cases} +1 & \text{if } y \text{ is a QR} \\ -1 & \text{if } y \text{ is a QNR} \end{cases}$$

Prop 11.2 in [KL]: For p>2 prime,

$$\left(\frac{y}{p}\right) = y^{\frac{p-1}{2}} \mod p$$