Key Distribution (1)

Yan Huang

Credit: David Evans (UVA)

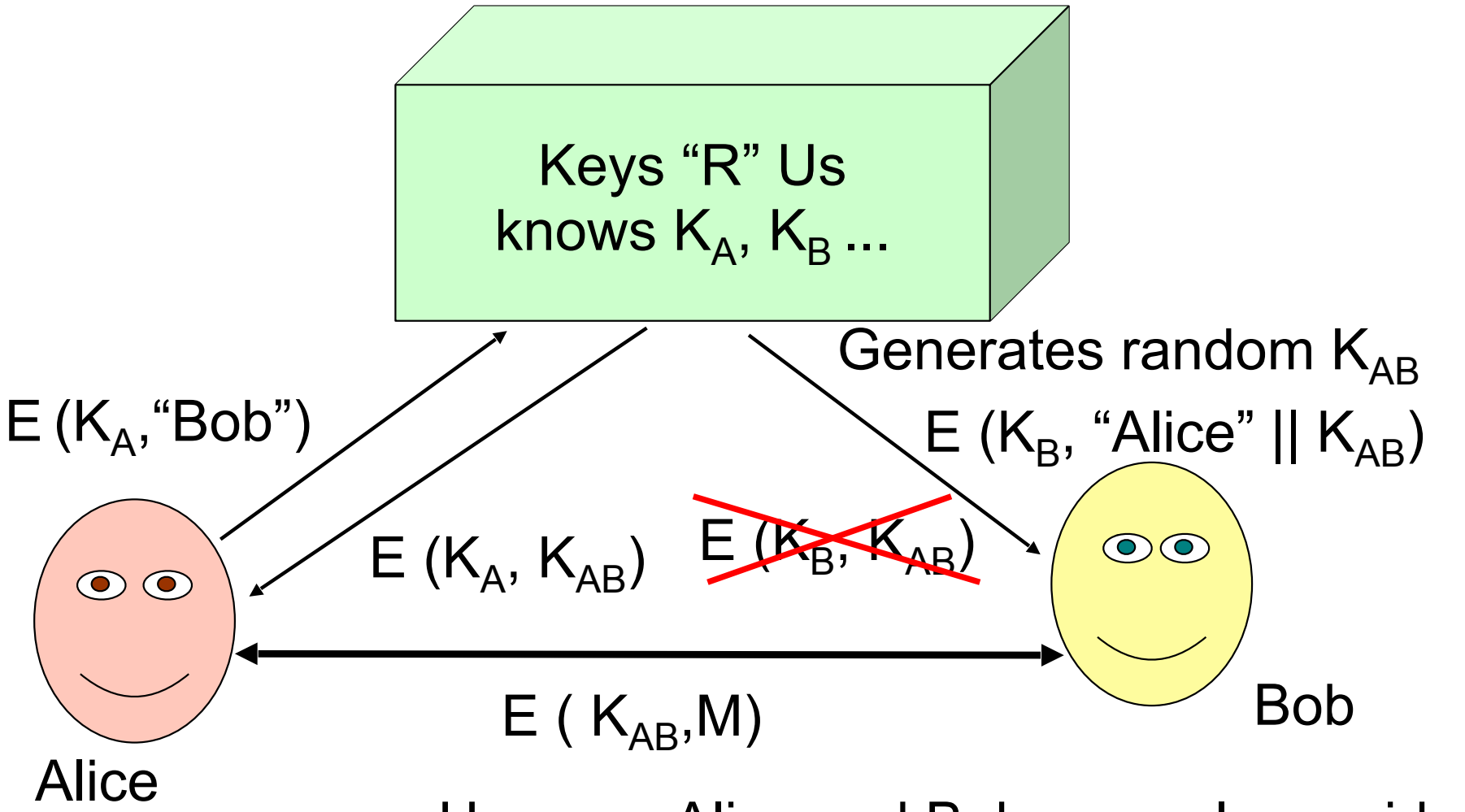
Symmetric-Key Cryptology

- Given a secure channel to transmit a shared secret key, symmetric cryptosystems amplify and time-shift that channel:
  - **[amplification]** transmit bigger secrets over an insecure channel (except one-time pad)
  - **[time-shifting]** transmit later secrets over an insecure channel
- But, the initial secure channel is required

Key Distribution

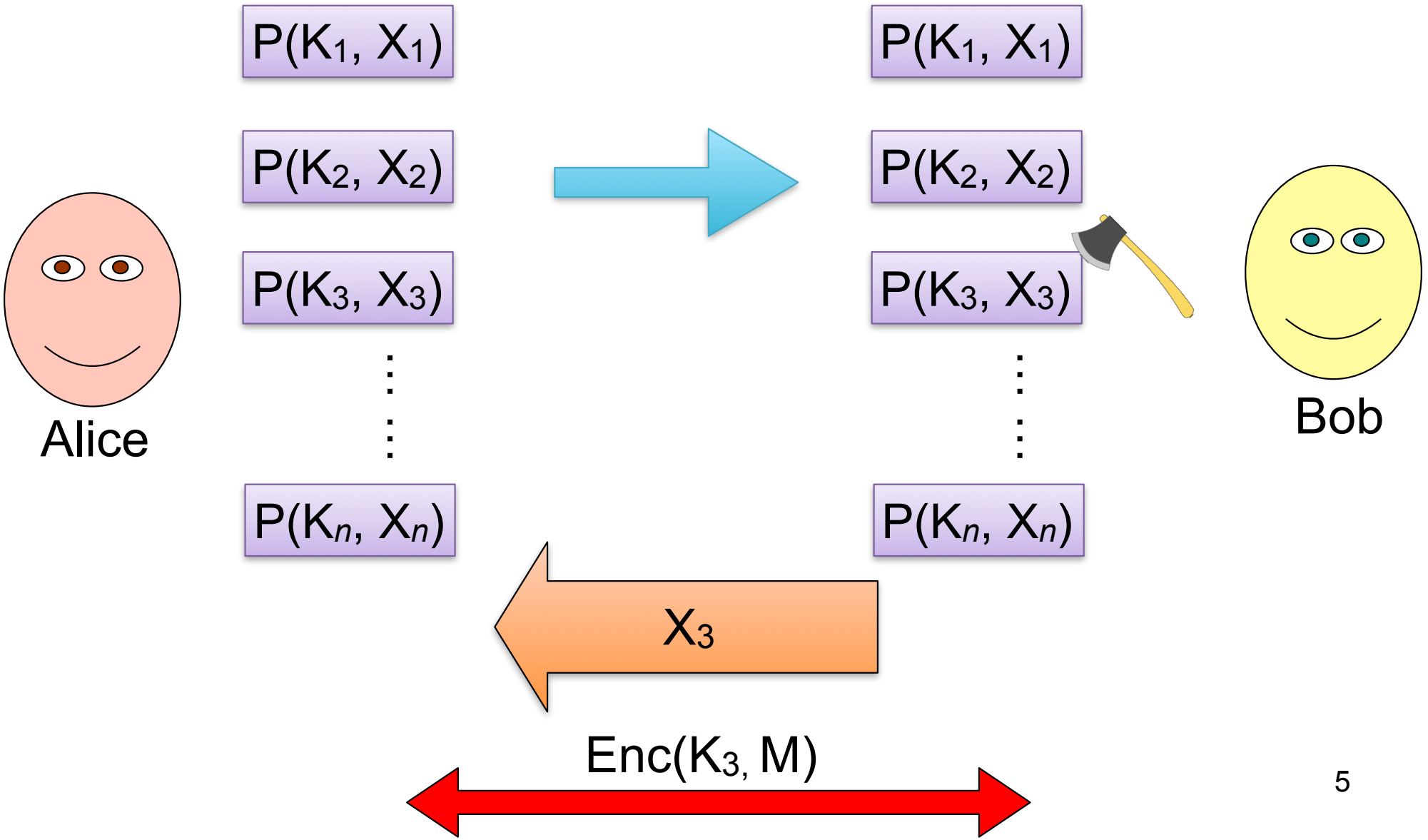
- All the cryptosystems we have seen depend on two parties having a shared secret
- Distributing secret keys is hard and expensive
  - $O(n^2)$ keys needed for n communicating parties
- Can two people communicate securely without having to meet first and establish a key? (Why do we care?)

Trust a Third Party



How can Alice and Bob securely provide their keys to Keys "R" Us?

Merkle's Puzzles



Merkle's Puzzles

- Ralph Merkle [1974]
- Alice generates 2^{20} messages: "This is puzzle x. The secret is y." (x and y are random numbers)
- Encrypts each message using symmetric cipher with a different key.
- Sends all encrypted messages to Bob

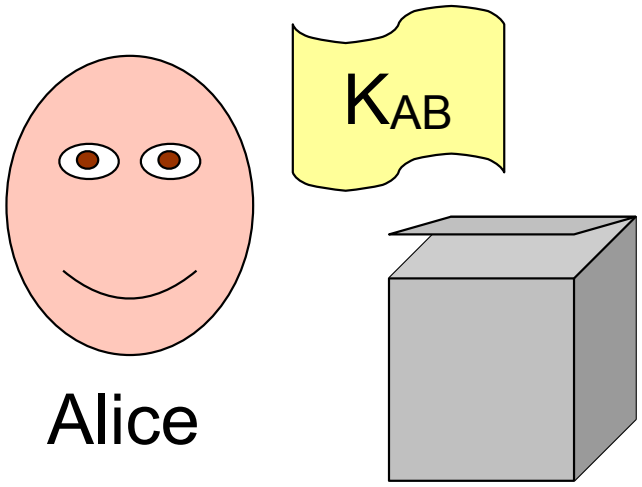
Merkle's Puzzles Key Agreement

- Bob chooses random message, performs brute-force attack to recover plaintext and secret y
- Bob sends x (in clear) to Alice
- Alice and Bob use y to encrypt messages

Is this secure?

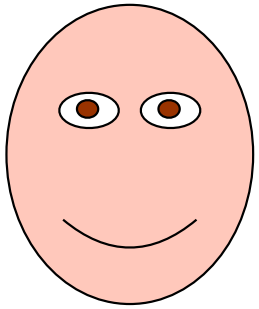
- Alice creates 2^{20} puzzles from DES cipher
  - ~2^{55} expected brute force work to break DES
- Eve: has to break expected 2^{19} to find which one matches x.
  - ~ 2^{19} * 2^{55} expected work
- Alice and Bob has to change keys frequently enough since it is less work to agree to a new key
- Why not increase the number of puzzles?

Padlocked Boxes



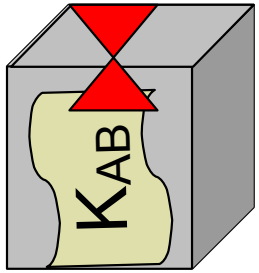
Padlocked Boxes

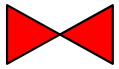
$E_A(M)$



Alice

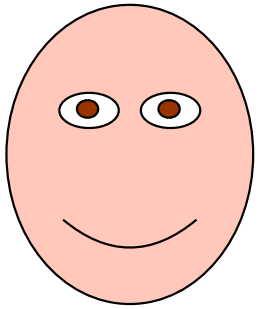
Alice's Padlock



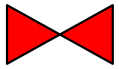


Alice's Padlock Key

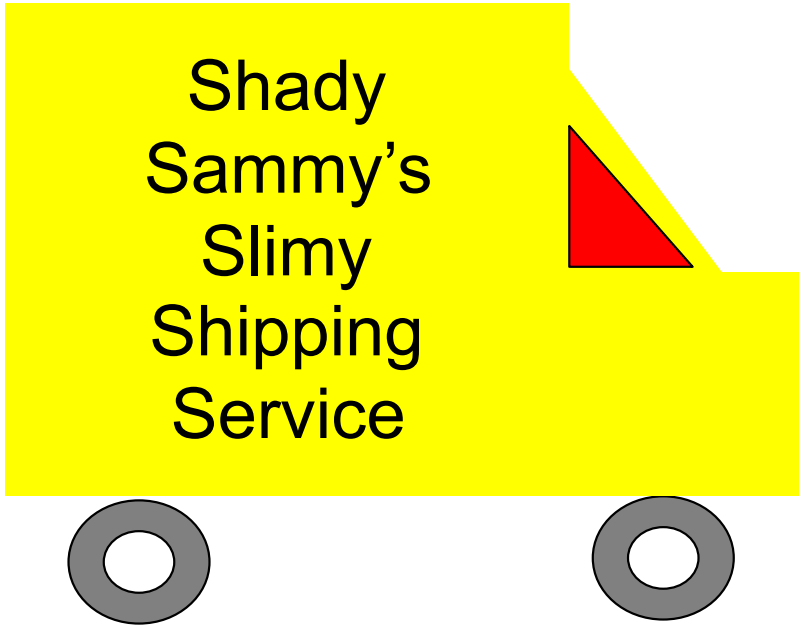
Padlocked Boxes



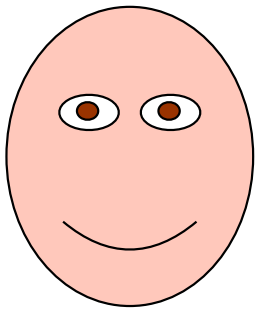
Alice



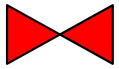
Alice's Padlock Key



Padlocked Boxes



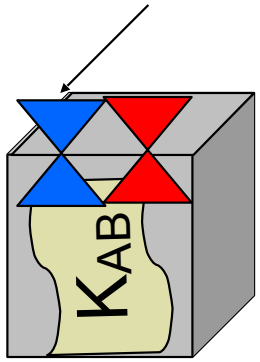
Alice

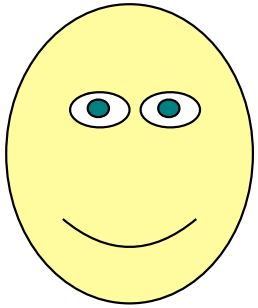


Alice's Padlock Key

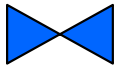
$E_B(E_A(M))$

Bob's Padlock





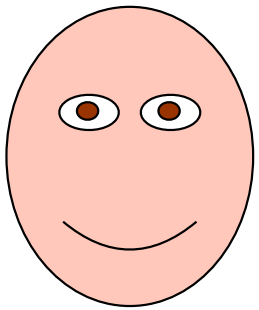
Bob



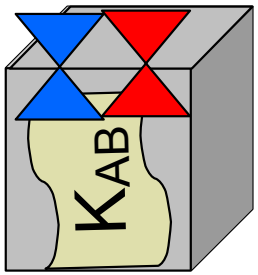
Bob's Padlock Key

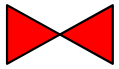
Padlocked Boxes

$E_B(E_A(M))$

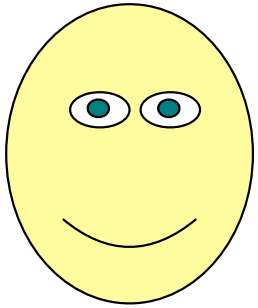


Alice

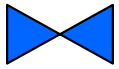




Alice's Padlock Key



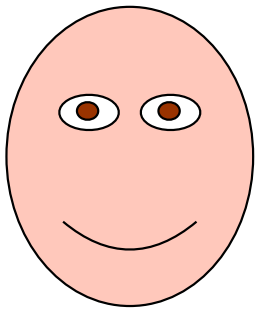
Bob



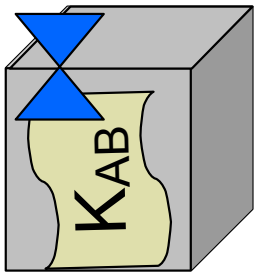
Bob's Padlock Key

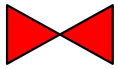
Padlocked Boxes

$$D_A(E_B(E_A(M))) = E_B(M)$$

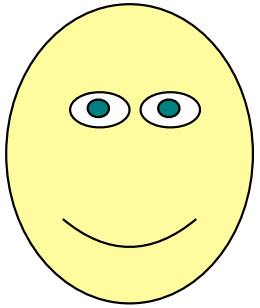


Alice

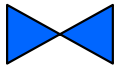




Alice's Padlock Key

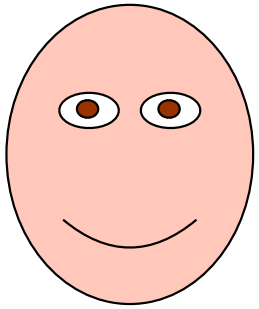


Bob



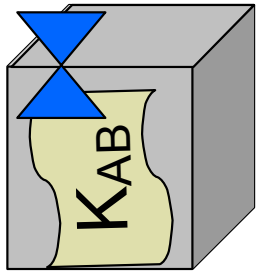
Bob's Padlock Key

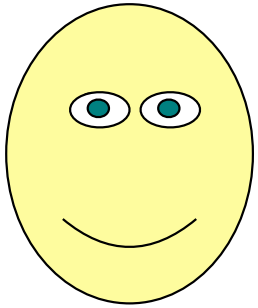
Padlocked Boxes



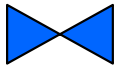
Alice

$E_B(M)$



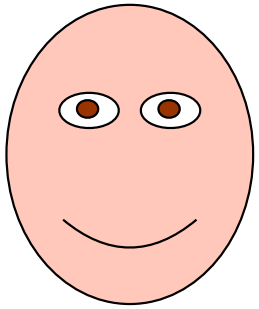


Bob

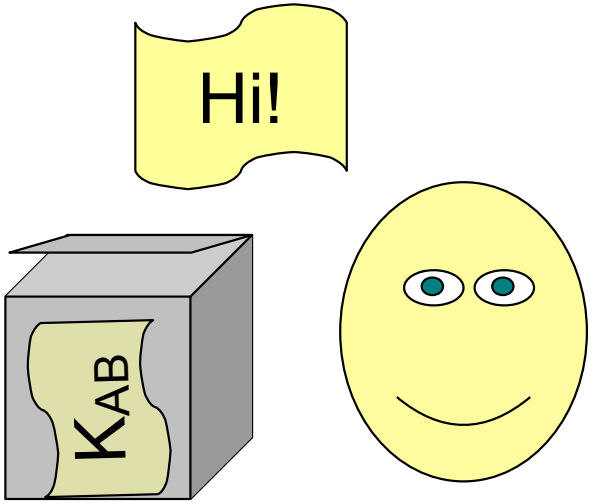


Bob's Padlock Key

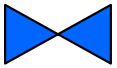
Padlocked Boxes



Alice



Bob



Bob's Padlock Key

Implement the Padlocked Box

- Does an AES-based encryption scheme suffice to implement the padlocked box?

Birth of Public Key Cryptosystems

- 1969 – ARPANet born: 4 sites
  - Whitfield Diffie starts thinking about strangers sending messages securely
- 1974 – Whitfield Diffie gives talk at IBM lab
  - Audience member mentions that Martin Hellman (Stanford prof) had spoke about key distribution
- That night – Diffie started driving 5000km to Palo Alto
- Diffie, Hellman and Ralph Merkle worked on key distribution problem

Whitfield Diffie

Whitfield Diffie and Martin E. Hellman, the recipients of the 2015 ACM A.M. Turing Award, for critical contributions to modern cryptography. The ability for two parties to communicate privately over a secure channel is fundamental for billions of people around the world.

We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

Diffie and Hellman, November 1976.

Charge

- Read the paper!
  - *New Directions in Cryptography*, W. Diffie and M. Hellman, IEEE Transactions on Information Theory, 1976
  - Go somewhere appropriate: this is perhaps the most important paper in past 30 years!