CS 6260 Applied Cryptography

Alexandra (Sasha) Boldyreva

Introduction, perfect (Shannon) secrecy

- All the information, including the link to the course web page is on T-Square.

Cryptography is very old and very new

- Crypto is an ancient discipline
  - Recall Julius Caesar, Enigma,...
- Crypto as a science (modern cryptography) has short but exciting history
  - Most of it happened in the last 30 years!
- This course will be an introduction to modern cryptography

Main goals of cryptography are

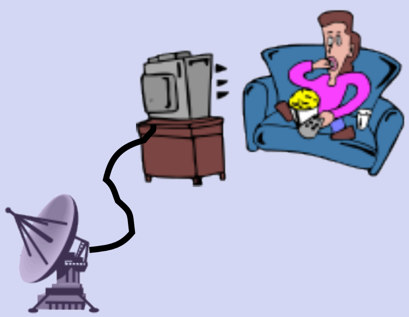
- data privacy
- data authenticity (message came from where it claims)
- data integrity (message has not been modified on the way)

in the digital world

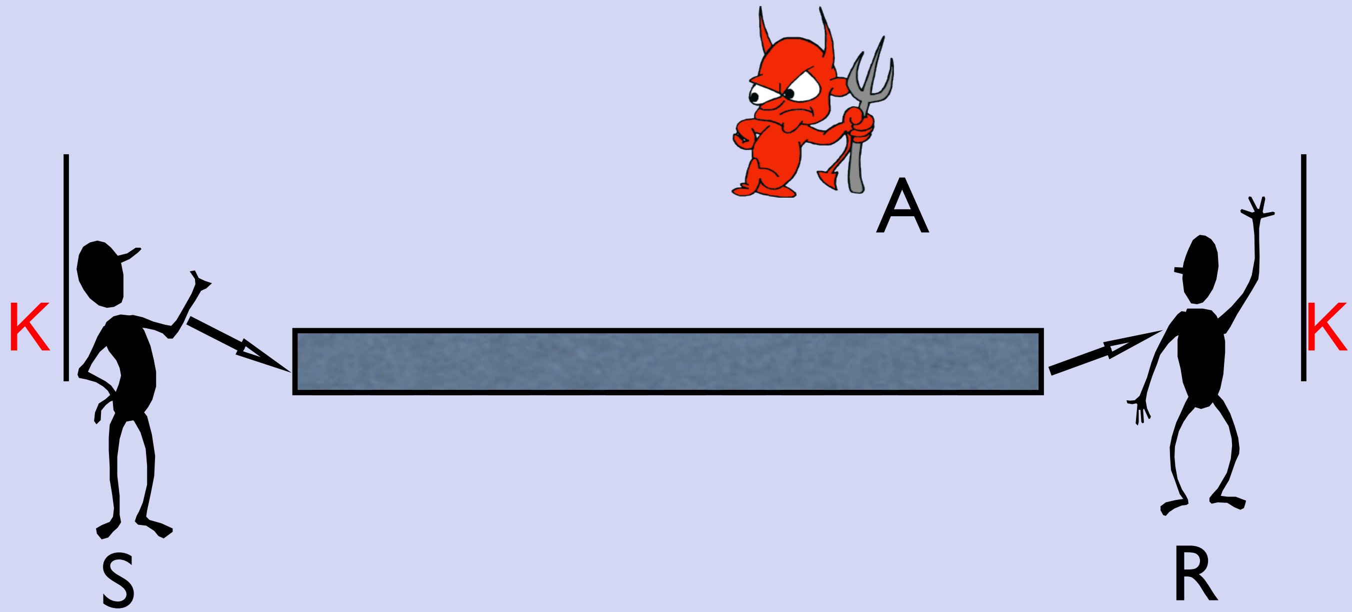
Who used some cryptography recently?

Crypto is used by most people when

- Doing on-line shopping and banking 
- Talking on a cell phone 
- Watching satellite TV and pay-per-view movies

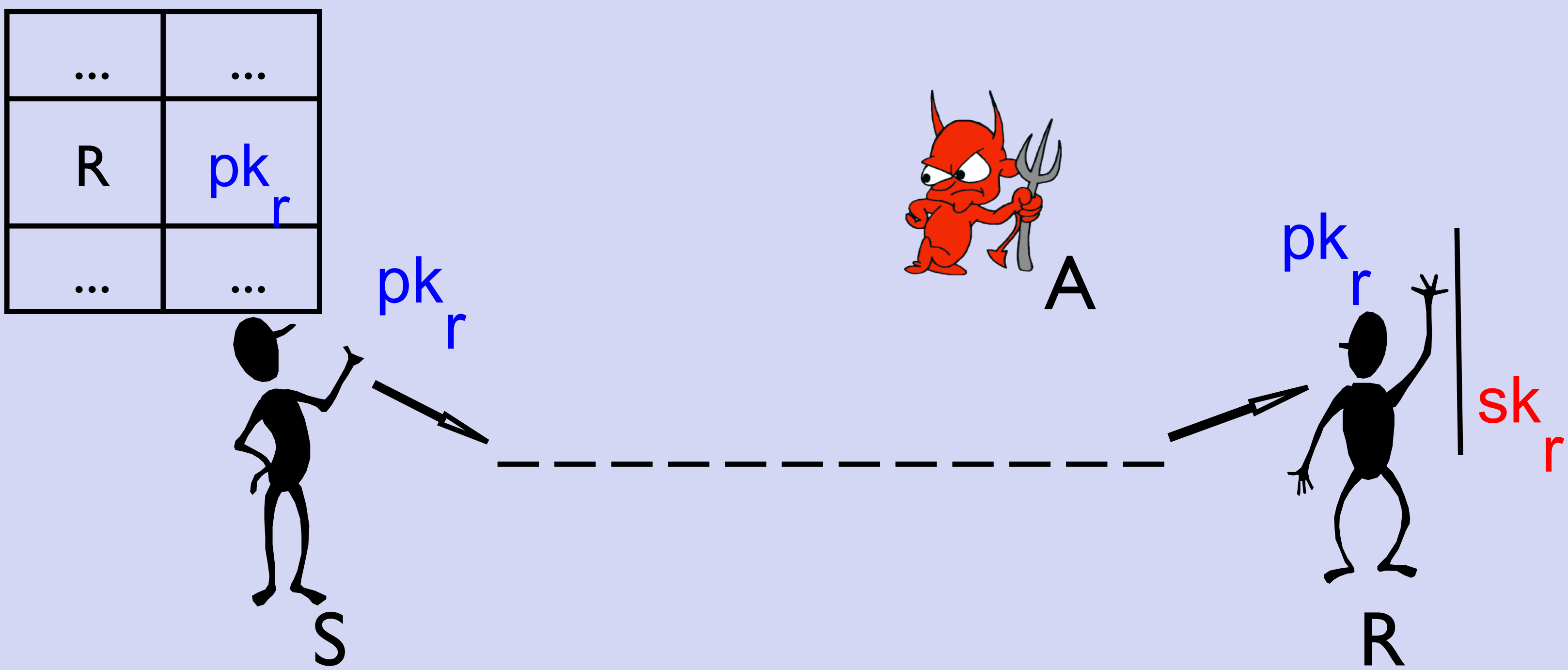


Players and settings



1. Symmetric-key setting

Players and settings



2. Asymmetric (public)-key setting

Goals and primitives

goal \ setting	symmetric-key	asymmetric-key
data privacy	symmetric (secret-key) encryption	asymmetric (public-key) encryption
data authenticity/ integrity	message authentication code (MAC)	digital signature scheme

How good is a scheme?

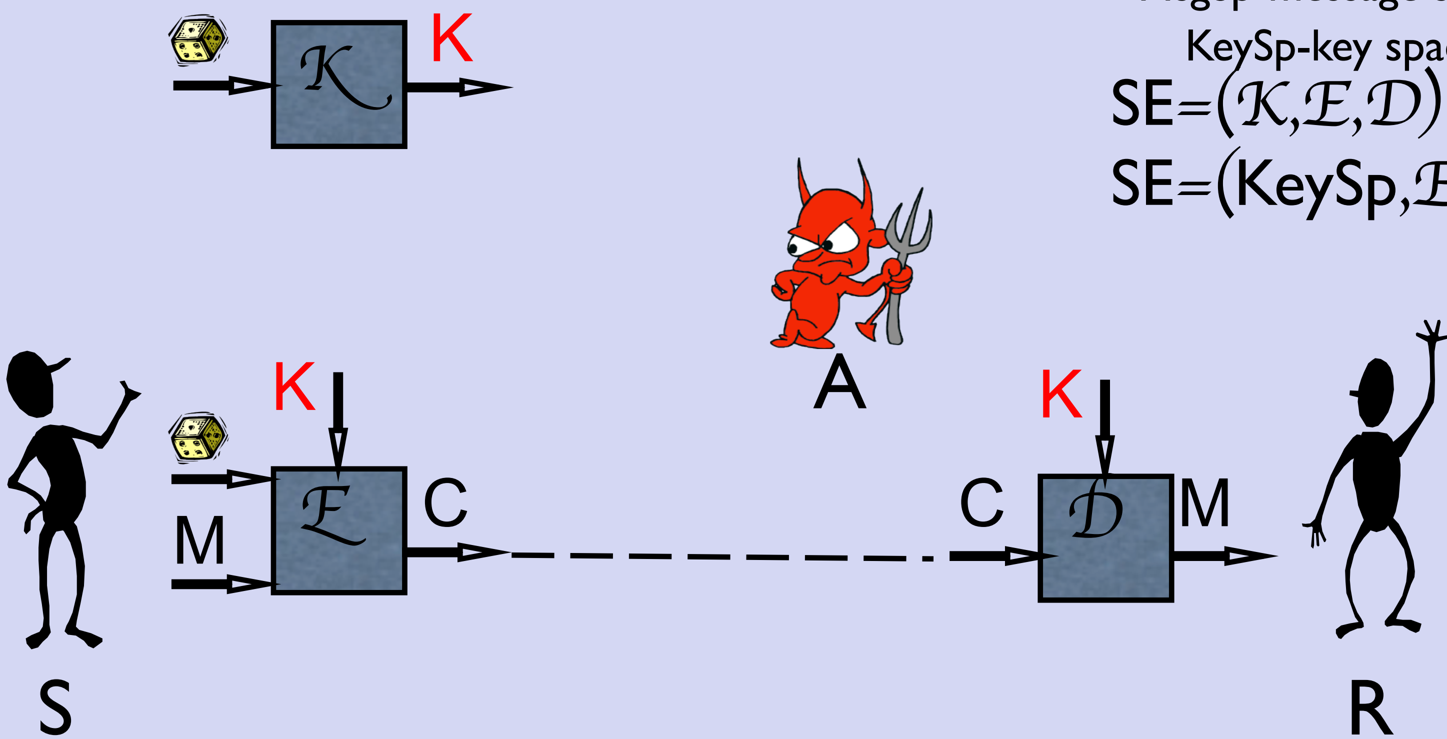
- "Trial-and-error" approach:
  1. Try to find an attack
  2. If an attack found then the scheme is insecure, fix the scheme, repeat step 1.
  3. If no attack found then ....?

- "Provable security" approach:
  - show that if an attack found (a scheme is insecure), then one can break some trusted assumption (e.g. factoring)
  - requires a definition of what "secure" means

Symmetric encryption schemes

- A scheme SE is specified by 3 algorithms $\mathcal{K},\mathcal{E},\mathcal{D}$.

MsgSp-message space
KeySp-key space
SE=$(\mathcal{K},\mathcal{E},\mathcal{D})$ or
SE=(KeySp,$\mathcal{E},\mathcal{D}$)



It is required that for every M∈MsgSp and every K∈KeySp,

$$\mathcal{D}(K, \mathcal{E}(K, M))=M$$

One Time Pad

- OneTimePad=($\mathcal{K}$,$\mathcal{E}$,$\mathcal{D}$), MsgSp=$\{0,1\}^n$:
  - $\mathcal{K}$: return a random n-bit string K (KeySp=$\{0,1\}^n$)
  - $\mathcal{E}$(K,M): C←M⊕K, return C
  - $\mathcal{D}$(K,C): M←C⊕K, return M
- Example: M=011111111011101

  K=110010011010100

  C=101101100001001
- A new key must be used to encrypt a new message

Perfect (Shannon) security

- Def 1. An encryption scheme SE=(K,E,D) is perfectly secure if for every probability distribution PD $\{0,1\}^n \to]0,1]$ on a MsgSp=$\{0,1\}^n$, for every ciphertext C and message M
  Pr[message is M | ciphertext is C] = PD(M)

  over the choices of K and a message that was encrypted

- Def 2. An encryption scheme SE=(K,E,D) is Shannon-secure if for every ciphertext C and messages M1,M2
  Pr[E(K1,M1)=C] = Pr[E(K2,M2)=C]

  over the choices of K1,K2

- Claim. Def 1 and Def 2 are equivalent, i.e. a scheme is perfectly secure iff it is Shannon-secure.

- Th.1 OneTimePad is a Shannon-secure encryption scheme.
  - Proof. Fix any ciphertext $C \in \{0,1\}^n$.
    For every M $Pr[E(K,M)=C] = Pr[K=M \oplus C] = 2^{-n}$

- Th.2 [Shannon's theorem, optimality of OneTimePad]
  If a scheme is Shannon-secure, than a key must be as long as the message we want to encrypt.
  - Proof. We prove that |KeySp| cannot be smaller than |MsgSp|.
    - Fix a ciphertext C (by picking M1,K1 and setting C=E(K1,M1)). Thus Pr[E(K,M1)=C]>0.
    - Assume there exists M2 such that Pr[D(K,C)=M2]=0.
    - By the correctness requirement Pr[E(K,M2)=C]=0. Therefore Pr[E(K,M1)=C]≠ Pr[E(K,M2)=C] that violates Shannon secrecy.
    - Thus for every M2∈MsgSp there exists K∈KeySp s.t. D(K,C)=M2, and thus |KeySp|>= |MsgSp|.

- Th.3 If a scheme is perfectly secure, than a key must be as long as the message we want to encrypt.
  - Proof. We prove that |KeySp| cannot be smaller than |MsgSp|.
    - Assume |KeySp|<|MsgSp|.
    - Fix C.
    - Let's count messages to which C can decrypt to under various keys:
    - $S=\{M_1,..M_{|KeySp|}\}$.
    - |S|<|MsgSp|, thus there exists M_i s.t. Pr[message is M_i|ciphertext is C]=0 while PD(M_i)>0.
    - A contradiction.

- So we cannot do better than OneTimePad. But it is impractical (needs a very long key). Is it the end?
  - Yes, of the information-theoretic crypto.
  - No, if we relax the security requirement and assume that adversaries are computationally bounded. We will also assume that
    - There are some “hard” problems
    - Secret keys are secret
    - All algorithms are public (Kerckhoff’s principle)
- We move to the area of computational-complexity crypto, that opens many of possibilities.