

CS 4803

Computer and Network Security

Alexandra (Sasha) Boldyreva
Cryptography. Introduction.

1

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!
- In this course we will study the basics of modern cryptography
- Modern cryptography means formal security models and definitions, proofs, etc.
- We won't always be formal and often just discuss the intuition.
- Those who want to learn more and are comfortable with theory may take CS 6260: Applied Cryptography.

2

Main goals of cryptography are

- data privacy (confidentiality)
- data authenticity (it came from where it claims)
- data integrity (it has not been modified on the way)
in the digital world

Who used some cryptography recently?

3

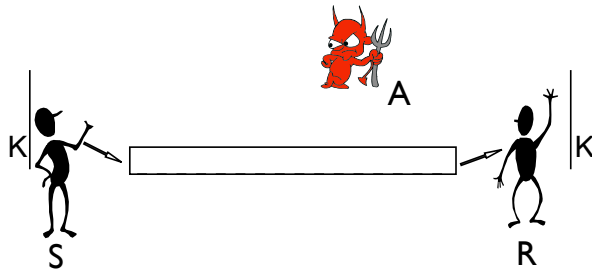
Crypto is used by most people when

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



4

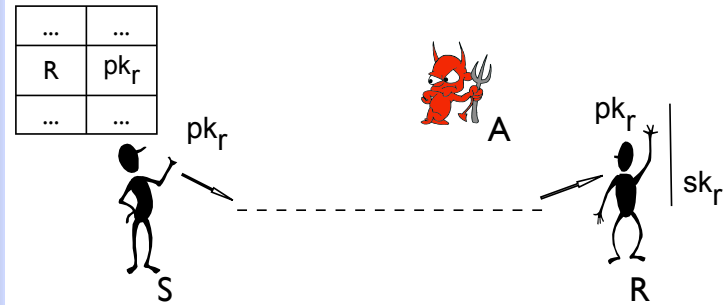
Players and settings



1. Symmetric-key setting

5

Players and settings



2. Asymmetric (public)-key setting

6

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

7

Symmetric vs public-key crypto

- Symmetric schemes are easier to construct and implement (less math is required)
- Symmetric schemes are faster (by 3-4 orders of magnitude)
- But how do parties agree on the shared key at the first place?

8

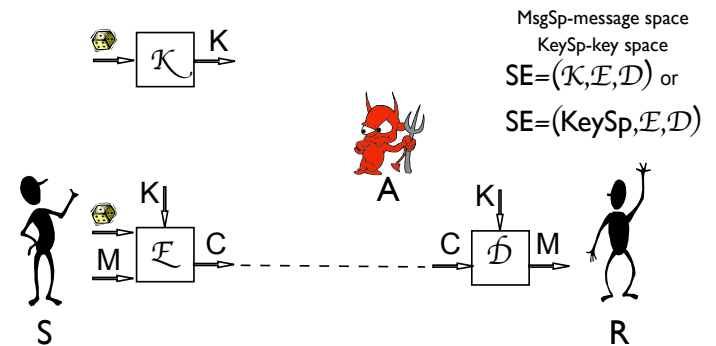
How good is a scheme?

- “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

9

Symmetric encryption schemes

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



It is required that for every $M \in \text{MsgSp}$ and every $K \in \text{KeySp}$,
 $\mathcal{D}(K, \mathcal{E}(K, M)) = M$

10

One Time Pad

- $\text{OneTimePad} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, $\text{MsgSp} = \{0,1\}^n$:
 - \mathcal{K} : return a random n-bit string K ($\text{KeySp} = \{0,1\}^n$)
 - $\mathcal{E}(K, M)$: $C \leftarrow M \oplus K$, return C
 - $\mathcal{D}(K, C)$: $M \leftarrow C \oplus K$, return M
- Example: $M = 011111111011101$
 $K = 110010011010100$
 $C = 101101100001001$
- As the name suggests, the scheme is to be used only once: a new key must be used to encrypt a new message.

11

Perfect (Shannon) security

- Def (informal). An encryption scheme $\text{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is perfectly secure if everything what can be learned about the message from a ciphertext can be learned without the ciphertext.
- Th.1 OneTimePad is a Shannon-secure encryption scheme.
- Th.2 [Shannon’s theorem, optimality of OneTimePad]
 If a scheme is perfectly secure, then the key space cannot be smaller than the message space (if $\text{KeySp} = \{0,1\}^k$ and $\text{MsgSp} = \{0,1\}^m$, then $k \geq m$ and a key must be as long as the message we want to encrypt).

12

- So we cannot do better than OneTimePad. But it is impractical (very fast, but we need a very long key). Is it the end? Yes, of the information-theoretic (unconditionally secure) crypto. No, if we relax the security requirement and assume that adversaries are computationally bounded. We will also assume that
 - Bad guys have limited computational power
 - There are some "hard" problems
 - Secret keys are secret
 - But we will NOT assume that algorithms are secret. All algorithms are public (Kerckhoff's principle). "Security by obscurity" is a bad idea!
- We move to the area of computational-complexity crypto, that opens a lot of possibilities.