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
2. Asymmetric (public)-key setting
### Goals and primitives

<table>
<thead>
<tr>
<th>Goal</th>
<th>Symmetric-key</th>
<th>Asymmetric-key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data privacy</td>
<td>symmetric (secret-key) encryption</td>
<td>asymmetric (public-key) encryption</td>
</tr>
<tr>
<td>Data authenticity/integrity</td>
<td>message authentication code (MAC)</td>
<td>digital signature scheme</td>
</tr>
</tbody>
</table>
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 $K, E, D$. 

\[ \text{SE} = (K, E, D) \text{ or } \text{SE} = (\text{KeySp}, E, D) \]

It is required that for every $M \in \text{MsgSp}$ and every $K \in \text{KeySp}$,

\[ D(K, E(K, M)) = M \]
One Time Pad

- OneTimePad=(K,E,D), MsgSp={0,1}^n:
  - K: return a random n-bit string K (KeySp={0,1}^n)
  - E(K,M): C←M⊕K, return C
  - 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 \( \{0,1\}^n \rightarrow [0,1] \) on a MsgSp=\( \{0,1\}^n \), for every ciphertext C and message M

\[ \Pr[\text{message is M | ciphertext is C}] = PD(M) \]

\( \text{over the choices of } K \text{ and a message that was encrypted} \)

• **Def 2.** An encryption scheme SE=(K,E,D) is Shannon-secure if for every ciphertext C and messages M1,M2

\[ \Pr[E(K_1,M_1)=C] = \Pr[E(K_2,M_2)=C] \]

\( \text{over the choices of } K_1,K_2 \)

• **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 $|\text{KeySp}|$ cannot be smaller than $|\text{MsgSp}|$.

- Fix a ciphertext $C$ (by picking $M_1, K_1$ and setting $C = E(K_1, M_1)$). Thus $\Pr[E(K, M_1) = C] > 0$.
- Assume there exists $M_2$ such that $\Pr[D(K, C) = M_2] = 0$.
- By the correctness requirement $\Pr[E(K, M_2) = C] = 0$. Therefore $\Pr[E(K, M_1) = C] \neq \Pr[E(K, M_2) = C]$ that violates Shannon secrecy.
- Thus for every $M_2 \in \text{MsgSp}$ there exists $K \in \text{KeySp}$ s.t. $D(K, C) = M_2$, and thus $|\text{KeySp}| \geq |\text{MsgSp}|$. 
• **Th.3** If a scheme is perfectly secure, then a key must be as long as the message we want to encrypt.

• **Proof.** We prove that $|\text{KeySp}|$ cannot be smaller than $|\text{MsgSp}|$.
  • Assume $|\text{KeySp}| < |\text{MsgSp}|$.
  • Fix C.
  • Let’s count messages to which C can decrypt to under various keys:
    • $S = \{M_1, \ldots, M_{|\text{KeySp}|}\}$.
    • $|S| < |\text{MsgSp}|$, thus there exists $M_i$ s.t.
      $\Pr[\text{message is } M_i | \text{ciphertext is C}] = 0$ while $\PrD(M_i) > 0$.
    • 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.