Department of
Computer Science and Engineering
计算机科学与工程系

CSE5014 CRYPTOGRAPHY AND NETWORK SECURITY

Dr. Qi Wang

Department of Computer Science and Engineering
Office: Room413, CoE South Tower
Email: wangqi@sustech.edu.cn

Principles of Mordern Cryptography

- Principle 1 – *Formal Definitions*
  - Precise, mathematical model and definition of what security means
- Principle 2 – *Precise Assumptions*
  - Clearly stated and unambiguous
- Principle 3 – *Proofs of Security*
  - Move away from “design-break-tweak”

Importance of definitions – design

- Definitions are essential for the design, analysis, and usage of crypto

Importance of definitions – design

- Definitions are essential for the design, analysis, and usage of crypto
- Developing a precise definition forces the designer to think about what they really want

Importance of definitions – design

- Definitions are essential for the design, analysis, and usage of crypto
- Developing a precise definition forces the designer to think about what they really want
  - What is essential and (sometimes more important) & what is not
  - Often reveals subtleties of the problem

Importance of definitions – design

- Definitions are essential for the design, analysis, and usage of crypto
- Developing a precise definition forces the designer to think about what they really want
  - What is essential and (sometimes more important) & what is not
  - Often reveals subtleties of the problem

If you don't understand what you want to achieve, how can you possibly know when (or if) you have achieved it?

Importance of definitions – analysis

- Definitions enable meaningful analysis, evaluation, and comparison of schemes

Importance of definitions – analysis

- Definitions enable meaningful analysis, evaluation, and comparison of schemes
  - Does a scheme satisfy the definition?
  - What definition does it satisfy?

Importance of definitions – analysis

- Definitions enable meaningful analysis, evaluation, and comparison of schemes
  - Does a scheme satisfy the definition?
  - What definition does it satisfy?

One scheme may be less efficient than another, yet satisfy a stronger security definition.

Importance of definitions – usage

- Definitions allow to understand the security guarantees provided by a scheme
- Enable schemes to be used as *components* of a larger system (modularity)
- Enable one scheme to be *substituted* for another if they satisfy the same definition

Assumptions

- With few exceptions, cryptography currently requires *computational assumptions*
  - At least until we prove $P \neq NP$ (even that would not be enough)

Assumptions

- With few exceptions, cryptography currently requires *computational assumptions*
  - At least until we prove $P \neq NP$ (even that would not be enough)
- Principle: any such assumptions should be made *explicit*

Importance of clear assumptions

- Allow researchers to (attempt to) *validate* assumptions by studying them
- Allow meaningful *comparison* between schemes based on different assumptions
  - Useful to understand minimal assumptions needed
- Practical implications if assumptions are wrong
- Enable proofs of security

Proofs of security

- Provide a rigorous *proof* that a construction satisfies a given *definition* under certian specified *assumptions*

- Proofs are crucial in crypto, where there is a malicious attacker trying to “break” the scheme

Limitations?

- Crypto remains partly an *art* as well

Limitations?

- Crypto remains partly an *art* as well

- Given a proof of security based on certain assumptions, we still need to instantiate the assumption.
  - Validity of various assumptions

Limitations?

- Crypto remains partly an *art* as well
- Given a proof of security based on certain assumptions, we still need to instantiate the assumption.
  - Validity of various assumptions
- Provably secure schemes can be broken!
  - If the definition does not correspond to the real-world threat model;
  - If the assumption is invalid;
  - If the implementation is flawed;

Defining secure encryption

- Crypto definitions (in general)

  Security guarantee/goal

  – What we want to achieve and/or what we want to prevent the attacker from achieving

  Threat model

  – What (real-world) capabilities the attacker is assumed to have

Private-key encryption

ciphertext

$c := Enc_k(m)$

Alice

m

message/plaintext

k

key

$c := Enc_k(m)$

encryption

Eve

(eavesdropper)

Bob

m'

k

key

$m' := Dec_k(c)$

decryption

Private-key encryption

- A *private-key encryption* scheme is defined by a message space $\mathcal{M}$ and algorithms (Gen, Enc, Dec):
  - Gen (*key-generation algorithm*): generates k
  - Enc (*encryption algorithm*): takes key k and message $m \in \mathcal{M}$ as input; outputs ciphertext c: $c \leftarrow Enc_k(m)$
  - Dec (*decryption algorithm*): takes key k and ciphertext c as input; outputs m': $m' := Dec_k(c)$

Threat models for encryption

- *Ciphertext-only attack*

  Known-plaintext attack

  Chosen-plaintext attack

  Chosen-ciphertext attack

Threat models for encryption

- *Ciphertext-only attack*
- *Known-plaintext attack*
- *Chosen-plaintext attack*
- *Chosen-ciphertext attack*

stronger

Probability review

- *Random variable* (r.v.): variable that takes on (discrete) values with certain probabilities

- *Probability distribution*: for an r.v. specifies the probabilities with which the variable takes on each possible value
  - Each probability must be between 0 and 1
  - The probabilities must sum to 1

Probability review

- *Event*: a particular occurrence in some experiment
  - Pr[E]: probability of event E

Probability review

- *Event*: a particular occurrence in some experiment
  - $\Pr[\mathrm{E}]$: probability of event E

- *Conditional probability*: probability that one event occurs, given that some other even occurred
  - $\Pr[\mathrm{A} \mid \mathrm{B}] = \Pr[A \text{ and } B]/\Pr[B]$

Probability review

- *Event*: a particular occurrence in some experiment
  - $\Pr[E]$: probability of event E

- *Conditional probability*: probability that one event occurs, given that some other even occurred
  - $\Pr[A \mid B] = \Pr[A \text{ and } B] / \Pr[B]$

- Two r.v.'s X, Y are *independent* if for all x, y:
  $\Pr[X = x \mid Y = y] = \Pr[X = x]$

Probability review

- *Law of total probability*: say $E_1, \ldots, E_n$ are a partition of all possibilities. Then for any A:
  $\Pr[A] = \sum_i \Pr[A \text{ and } E_i] = \sum_i \Pr[A \mid E_i] \cdot \Pr[E_i]$

Probability review

- *Law of total probability*: say $E_1, \ldots, E_n$ are a partition of all possibilities. Then for any A:
  $\Pr[A] = \sum_i \Pr[A \text{ and } E_i] = \sum_i \Pr[A \mid E_i] \cdot \Pr[E_i]$

- Notation
  - $\mathcal{K}$ (*key space*): set of all possible keys
  - $\mathcal{M}$ (*plaintext space*): set of all possible plaintexts
  - $\mathcal{C}$ (*ciphertext space*): set of all possible ciphertexts

Probability distributions

- M: the r.v. denoting the value of the message
  - M ranges over $\mathcal{M}$
  - This reflects the likelihood of different messages being sent by the parties, given the attacker's prior knowledge

Probability distributions

- M: the r.v. denoting the value of the message
  - M ranges over $\mathcal{M}$
  - This reflects the likelihood of different messages being sent by the parties, given the attacker's prior knowledge
  - For example,

$$\Pr[M = \text{“attack today”}] = 0.7$$

$$\Pr[M = \text{“don't attack”}] = 0.3$$

Probability distributions

- K: the r.v. denoting the key
  - K ranges over $\mathcal{K}$

Probability distributions

- K: the r.v. denoting the key
  - K ranges over $\mathcal{K}$
- Fix some encryption scheme (Gen, Enc, Dec)
  - Gen defines a probability distribution for K:

$$\Pr[K = k] = \Pr[Gen \text{ outputs key } k]$$

Probability distributions

- Random variables M and K are independent
  - i.e., the message that a party sends does not depend on the key used to encrypt that message

Probability distributions

- Random variables M and K are independent
  - i.e., the message that a party sends does not depend on the key used to encrypt that message
- Fix some encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$, and some distribution for M. Consider the following (randomized) experiment:
  1. Choose a message m, according to the given distribution
  2. Generate a key k using Gen
  3. Compute $c \leftarrow Enc_k(m)$

Probability distributions

- Random variables M and K are independent
  - i.e., the message that a party sends does not depend on the key used to encrypt that message
- Fix some encryption scheme (Gen, Enc, Dec), and some distribution for M. Consider the following (randomized) experiment:
  1. Choose a message m, according to the given distribution
  2. Generate a key k using Gen
  3. Compute $c \leftarrow Enc_k(m)$
- This defines a distribution on the ciphertext. Let C be an r.v. denoting the value of the ciphertext in this experiment

Example 1

- Consider the shift cipher
  - So for all $k \in \{0, \ldots, 25\}$, $\Pr[K = k] = 1/26$

  Say $\Pr[M = \text{‘a’}] = 0.7$, $\Pr[M = \text{‘z’}] = 0.3$

  What is $\Pr[C = \text{‘b’}]$?

Example 1

- Consider the shift cipher
  - So for all $k \in \{0, \ldots, 25\}$, $\Pr[K = k] = 1/26$

  Say $\Pr[M = \text{‘a’}] = 0.7$, $\Pr[M = \text{‘z’}] = 0.3$

  What is $\Pr[C = \text{‘b’}]$?

  - Either $M = \text{‘a’}$ and $K = 1$, or $M = \text{‘z’}$ and $K = 2$

Example 1

- Consider the shift cipher
  - So for all $k \in \{0, \ldots, 25\}$, $\Pr[K = k] = 1/26$

  Say $\Pr[M = \text{'a'}] = 0.7$, $\Pr[M = \text{'z'}] = 0.3$

  What is $\Pr[C = \text{'b'}]$?

  - Either $M = \text{'a'}$ and $K = 1$, or $M = \text{'z'}$ and $K = 2$
  - $\Pr[C = \text{'b'}] = \Pr[M = \text{'a'}] \cdot \Pr[K = 1] + \Pr[M = \text{'z'}] \cdot \Pr[K = 2]$

$$= 0.7 \cdot (1/26) + 0.3 \cdot (1/26)$$
$$= 1/26$$

Example 2

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{'one'}] = 1/2$, $\Pr[M = \text{'ten'}] = 1/2$

  $\Pr[C = \text{'rqh'}] = ?$

Example 2

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{`one'}] = 1/2$, $\Pr[M = \text{`ten'}] = 1/2$

  $\Pr[C = \text{`rqh'}] =?$

  $$= \Pr[C = \text{`rqh'} | M = \text{`one'}] \cdot \Pr[M = \text{`one'}] + \Pr[C = \text{`rqh'} \; | M = \text{`ten'}] \cdot \Pr[M = \text{`ten'}]$$

  $$= 1/26 \cdot 1/2 + 0 \cdot 1/2 = 1/52$$

Goal of secure encryption?

- How would you define what it means for encrytpion scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over message space $\mathcal{M}$ to be secure?
  - Against a (single) ciphertext-only attack
  - Suppose that $k \in \{0,1\}^n, m \in \{0,1\}^\ell, c \in \{0,1\}^L$

Secure encryption?

- "Impossible for the attacker to learn the key"

Secure encryption?

- "Impossible for the attacker to learn the key"
  - The key is a means to an end, not the end itself
  - Necessary (to some extent) but not sufficient
  - Easy to design an encryption scheme that hides the key completely, but is insecure

Secure encryption?

- "Impossible for the attacker to learn the key"
  - The key is a means to an end, not the end itself
  - Necessary (to some extent) but not sufficient
  - Easy to design an encryption scheme that hides the key completely, but is insecure

Definition 1.1 *Security of encryption* (Ver. 1). An encryption scheme (Gen, Enc, Dec) is *n-secure* if no matter what method Eve employs, the probability that she can recover the key k from the ciphertext c is at most 2^{-n}.

Secure encryption?

- "Impossible for the attacker to learn the key"
  - The key is a means to an end, not the end itself
  - Necessary (to some extent) but not sufficient
  - Easy to design an encryption scheme that hides the key completely, but is insecure

Definition 1.1 *Security of encryption* (Ver. 1). An encryption scheme (Gen, Enc, Dec) is *n-secure* if no matter what method Eve employs, the probability that she can recover the key k from the ciphertext c is at most 2^{-n}.

Definition 1.1 is too weak!

Secure encryption?

- "Impossible for the attacker to learn the key"
  - The key is a means to an end, not the end itself
  - Necessary (to some extent) but not sufficient
  - Easy to design an encryption scheme that hides the key completely, but is insecure

Definition 1.1 *Security of encryption* (Ver. 1). An encryption scheme (Gen, Enc, Dec) is *n-secure* if no matter what method Eve employs, the probability that she can recover the key k from the ciphertext c is at most 2^{-n}.

Definition 1.1 is too weak!
Consider: the secret key k is chosen at random in $\{0,1\}^n$ but our encryption scheme is simply $Enc_k(x) = x$ and $Dec_k(y) = y$.

Secure encryption?

- **Lemma 1.2** Let (Gen, Enc, Dec) be the encryption scheme above. For every function $Eve : \{0,1\}^\ell \to \{0,1\}^n$ and for every $x \in \{0,1\}^\ell$, the probability that $Eve(Enc_k(x)) = k$ is exactly 2^{-n}.

Secure encryption?

- **Lemma 1.2** Let (Gen, Enc, Dec) be the encryption scheme above. For every function $Eve : \{0,1\}^{\ell} \to \{0,1\}^{n}$ and for every $x \in \{0,1\}^{\ell}$, the probability that $Eve(Enc_k(x)) = k$ is exactly 2^{-n}.

  Proof. This follows because $Enc_k(x) = x$ and hence $Eve(Enc_k(x)) = Eve(x)$ which is some fixed value $k' \in \{0,1\}^{n}$ independent of k. Hence the probability that $k = k'$ is 2^{-n}.

Secure encryption?

- **Lemma 1.2** Let (Gen, Enc, Dec) be the encryption scheme above. For every function $Eve : \{0,1\}^\ell \to \{0,1\}^n$ and for every $x \in \{0,1\}^\ell$, the probability that $Eve(Enc_k(x)) = k$ is exactly 2^{-n}.

  Proof. This follows because $Enc_k(x) = x$ and hence $Eve(Enc_k(x)) = Eve(x)$ which is some fixed value $k' \in \{0,1\}^n$ independent of k. Hence the probability that $k = k'$ is 2^{-n}.

  Problem for Ver. 1: Could be hard to learn key, but easy to learn message.

Secure encryption?

- **Definition 1.3** *Security of encryption* (Ver. 2). An encryption scheme (Gen, Enc, Dec) is *n-secure* if for every message m no matter what method Eve employs, the probability that she can recover x from the ciphertext c is at most 2^{-n}.

Secure encryption?

- **Definition 1.3** *Security of encryption* (Ver. 2). An encryption scheme (Gen, Enc, Dec) is *n-secure* if for every message m no matter what method Eve employs, the probability that she can recover x from the ciphertext c is at most 2^{-n}.

  Problem for Ver. 2: Too strong, for "every message", it is impossible to achieve!

Secure encryption?

- **Definition 1.3** *Security of encryption* (Ver. 2). An encryption scheme (Gen, Enc, Dec) is *n-secure* if for every message m no matter what method Eve employs, the probability that she can recover x from the ciphertext c is at most 2^{-n}.

  Problem for Ver. 2: Too strong, for "every message", it is impossible to achieve!

  Example: $Eve(Enc_k(x)) = 0^\ell$ for all x
  $x = 0^\ell$

Secure encryption?

- **Definition 1.4** *Security of encryption* (Ver. 3). An encryption scheme (Gen, Enc, Dec) is *n-secure* if no matter what method Eve employs, if x is chosen at random from $\{0,1\}^\ell$, the probability that she can recover x from the ciphertext c is at most 2^{-n}.

Secure encryption?

- **Definition 1.4** *Security of encryption* (Ver. 3). An encryption scheme (Gen, Enc, Dec) is *n-secure* if no matter what method Eve employs, if x is chosen at random from $\{0,1\}^\ell$, the probability that she can recover x from the ciphertext c is at most 2^{-n}.

  Problem for Ver. 3: Still weak!

Secure encryption?

- **Definition 1.4** *Security of encryption* (Ver. 3). An encryption scheme (Gen, Enc, Dec) is *n-secure* if no matter what method Eve employs, if x is chosen at random from $\{0,1\}^\ell$, the probability that she can recover x from the ciphertext c is at most 2^{-n}.

  Problem for Ver. 3: Still weak!

  Consider an encryption that hides the last $\ell/2$ bits of the message, but completely reveals the first $\ell/2$ bits. The probability of guessing a random message is $2^{-\ell/2}$, and so it would be $\ell/2$-secure.

Secure encryption?

- *Perfect secrecy* (informal)
  - "Regardless of any *prior* information the attacker has about the plaintext, the ciphertext should leak *no additional* information about the plaintext"

Secure encryption?

- *Perfect secrecy* (informal)
  - "Regardless of any *prior* information the attacker has about the plaintext, the ciphertext should leak *no additional* information about the plaintext"
  - Attacker's information about the plaintext $=$ attacker-known *distribution* of M

Secure encryption?

- *Perfect secrecy* (informal)
  - "Regardless of any *prior* information the attacker has about the plaintext, the ciphertext should leak *no additional* information about the plaintext"
  - Attacker's information about the plaintext = attacker-known *distribution* of M
  - Perfect secrecy means that observing the ciphertext should not change the attacker's knowledge about the distribution of M

Secure encryption?

- *Perfect secrecy* (formal)
  Definition 1.5 An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *perfectly secure* if for every distribution over $\mathcal{M}$, every $m \in \mathcal{M}$, and every $c \in \mathcal{C}$ with $\Pr[C = c] > 0$, it holds that

$$\Pr[M = m | C = c] = \Pr[M = m]$$

Secure encryption?

- *Perfect secrecy* (formal)

  Definition 1.5 An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *perfectly secure* if for every distribution over $\mathcal{M}$, every $m \in \mathcal{M}$, and every $c \in \mathcal{C}$ with $\Pr[C = c] > 0$, it holds that

  $$\Pr[M = m | C = c] = \Pr[M = m]$$

  Key point: The ciphertext c reveals zero additional information about the plaintext m.

Example 3

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{`one'}] = 1/2$, $\Pr[M = \text{`ten'}] = 1/2$

  Take $m = $ 'ten' and $c = $ 'rqh'

Example 3

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{'one'}] = 1/2$, $\Pr[M = \text{'ten'}] = 1/2$

  Take $m = \text{'ten'}$ and $c = \text{'rqh'}$

  $\Pr[M = \text{'ten'} | C = \text{'rqh'}] = ?$

Example 3

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{'one'}] = 1/2$, $\Pr[M = \text{'ten'}] = 1/2$

  Take $m = \text{'ten'}$ and $c = \text{'rqh'}$

  $\Pr[M = \text{'ten'} | C = \text{'rqh'}] = ?$

  $= 0$

  $\neq \Pr[M = \text{'ten'}]$

Example 3

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{`one'}] = 1/2$, $\Pr[M = \text{`ten'}] = 1/2$

  Take $m = \text{`ten'}$ and $c = \text{`rqh'}$

  $$\Pr[M = \text{`ten'} | C = \text{`rqh'}] = ?$$

  $$= 0$$

  $$\neq \Pr[M = \text{`ten'}]$$

- *Bayes's theorem*
  $$\Pr[A \mid B] = \Pr[B \mid A] \cdot \Pr[A] / \Pr[B]$$

Example 4

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{'hi'}] = 0.3$, $\Pr[M = \text{'no'}] = 0.2$,
  $\Pr[M = \text{'in'}] = 0.5$

  Take $m = \text{'hi'}$ and $c = \text{'xy'}$

Example 4

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{`hi'}] = 0.3$, $\Pr[M = \text{`no'}] = 0.2$,
  $\Pr[M = \text{`in'}] = 0.5$

  Take $m = \text{`hi'}$ and $c = \text{`xy'}$

  $\Pr[M = \text{`hi'} | C = \text{`xy'}] = ?$

Example 4

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{`hi'}] = 0.3$, $\Pr[M = \text{`no'}] = 0.2$,
  $\Pr[M = \text{`in'}] = 0.5$

  Take $m = \text{`hi'}$ and $c = \text{`xy'}$
  $\Pr[M = \text{`hi'} | C = \text{`xy'}] = ?$
  $= \Pr[C = \text{`xy'} | M = \text{`hi'}] \cdot \Pr[M = \text{`hi'}] / \Pr[C = \text{`xy'}]$

Example 4

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{`hi'}] = 0.3$, $\Pr[M = \text{`no'}] = 0.2$,
  $\Pr[M = \text{`in'}] = 0.5$

  Take $m = \text{`hi'}$ and $c = \text{`xy'}$
  $\Pr[M = \text{`hi'} | C = \text{`xy'}] = ?$
  $= \Pr[C = \text{`xy'} | M = \text{`hi'}] \cdot \Pr[M = \text{`hi'}] / \Pr[C = \text{`xy'}]$

  $\Pr[C = \text{`xy'} | M = \text{`hi'}] = 1/26$

Example 4

- Consider the shift cipher, and the distribution

  $\Pr[M = \text{'hi'}] = 0.3$, $\Pr[M = \text{'no'}] = 0.2$,
  $\Pr[M = \text{'in'}] = 0.5$

  Take $m = \text{'hi'}$ and $c = \text{'xy'}$

  $$\Pr[M = \text{'hi'} | C = \text{'xy'}] = ?$$
  $$= \Pr[C = \text{'xy'} | M = \text{'hi'}] \cdot \Pr[M = \text{'hi'}] / \Pr[C = \text{'xy'}]$$

  $$\Pr[C = \text{'xy'} | M = \text{'hi'}] = 1/26$$
  $$\Pr[C = \text{'xy'}]$$
  $$= \Pr[C = \text{'xy'} | M = \text{'hi'}] \cdot 0.3 + \Pr[C = \text{'xy'} | M = \text{'no'}] \cdot 0.2$$
  $$+ \Pr[C = \text{'xy'} | M = \text{'in'}] \cdot 0.5$$
  $$= (1/26) \cdot 0.3 + (1/26) \cdot 0.2 + 0 \cdot 0.5 = 1/52$$

Example 4

- Consider the shift cipher, and the distribution
  $\Pr[M = \text{'hi'}] = 0.3$, $\Pr[M = \text{'no'}] = 0.2$,
  $\Pr[M = \text{'in'}] = 0.5$

  Take $m = \text{'hi'}$ and $c = \text{'xy'}$

  $$\begin{aligned}&\Pr[M = \text{'hi'} | C = \text{'xy'}] =?\\ &= \Pr[C = \text{'xy'} | M = \text{'hi'}] \cdot \Pr[M = \text{'hi'}] / \Pr[C = \text{'xy'}]\\ &= (1/26) \cdot 0.3/(1/52) = 0.6 \neq \Pr[M = \text{'hi'}]\end{aligned}$$

  $$\begin{aligned}&\Pr[C = \text{'xy'} | M = \text{'hi'}] = 1/26\\ &\Pr[C = \text{'xy'}]\\ &= \Pr[C = \text{'xy'} | M = \text{'hi'}] \cdot 0.3 + \Pr[C = \text{'xy'} | M = \text{'no'}] \cdot 0.2\\ &\quad + \Pr[C = \text{'xy'} | M = \text{'in'}] \cdot 0.5\\ &= (1/26) \cdot 0.3 + (1/26) \cdot 0.2 + 0 \cdot 0.5 = 1/52\end{aligned}$$

Perfect secrecy

- The shift cipher is not *perfectly secure*!

Perfect secrecy

- The shift cipher is not *perfectly secure*!

Definition 1.5 An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *perfectly secure* if for every distribution over $\mathcal{M}$, every $m \in \mathcal{M}$, and every $c \in \mathcal{C}$ with $\Pr[C = c] > 0$, it holds that

$$\Pr[M = m | C = c] = \Pr[M = m]$$

Perfect secrecy

- The shift cipher is not *perfectly secure*!

Definition 1.5 An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *perfectly secure* if for every distribution over $\mathcal{M}$, every $m \in \mathcal{M}$, and every $c \in \mathcal{C}$ with $\Pr[C = c] > 0$, it holds that

$$\Pr[M = m | C = c] = \Pr[M = m]$$

Equivalently, for every set $M \subseteq \{0,1\}^\ell$ of plaintexts, and for every strategy used by Eve, if we choose at random $x \in M$ and a random key $k \in \{0,1\}^n$, then the probability that Eve guesses x after seeing $Enc_k(x)$ is at most $1/|M|$, i.e.,

$$\Pr[Eve(Enc_k(x)) = x] \leq 1/|M|$$

Perfect secrecy

- Another two equivalent definitions

Perfect secrecy

- Another two equivalent definitions

  Definition 1.6 *Perfect secrecy*. An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *perfectly secure* if and only if for every two distinct plaintexts $\{x_0, x_1\} \in \mathcal{M}$, and for every strategy used by Eve, if we choose at random $b \in \{0, 1\}$ and a random key $k \in \{0, 1\}^n$, then the probability that Eve guesses x_b after seeing the ciphertext $c = Enc_k(x_b)$ is at most $1/2$.

Perfect secrecy

- Another two equivalent definitions

  Definition 1.6 *Perfect secrecy*. An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *perfectly secure* if and only if for every two distinct plaintexts $\{x_0, x_1\} \in \mathcal{M}$, and for every strategy used by Eve, if we choose at random $b \in \{0, 1\}$ and a random key $k \in \{0, 1\}^n$, then the probability that Eve guesses x_b after seeing the ciphertext $c = Enc_k(x_b)$ is at most $1/2$.

  Definition 1.7 *Perfect secrecy*. Two probability distributions X, Y over $\{0, 1\}^\ell$ are *identical*, denoted by $X \equiv Y$, if for every $y \in \{0, 1\}^\ell$, $\Pr[X = y] = \Pr[Y = y]$. An encryption scheme (Gen, Enc, Dec) is *perfectly secure* if for every pair of plaintexts x, x', we have $Enc_{U_n}(x) \equiv Enc_{U_n}(x')$.

Perfect secrecy

- Another two equivalent definitions

Definition 1.6 *Perfect secrecy*. An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *perfectly secure* if and only if for every two distinct plaintexts $\{x_0, x_1\} \in \mathcal{M}$, and for every strategy used by Eve, if we choose at random $b \in \{0,1\}$ and a random key $k \in \{0,1\}^n$, then the probability that Eve guesses x_b after seeing the ciphertext $c = Enc_k(x_b)$ is at most $1/2$.

Definition 1.7 *Perfect secrecy*. Two probability distributions X, Y over $\{0,1\}^\ell$ are *identical*, denoted by $X \equiv Y$, if for every $y \in \{0,1\}^\ell$, $\Pr[X = y] = \Pr[Y = y]$. An encryption scheme (Gen, Enc, Dec) is *perfectly secure* if for every pair of plaintexts x, x', we have $Enc_{U_n}(x) \equiv Enc_{U_n}(x')$.

$\mathcal{Q}$: Does this mean that for every k, $Enc_k(x) = Enc_k(x')$?

- **Theorem 1.8** (Two-to-Many Theorem) The scheme (Gen, Enc, Dec) is *perfectly secure* if and only if

$$Pr[Eve(Enc_k(x_0)) = x_0] \leq 1/2.$$

Perfect Secrecy

- **Theorem 1.8** (Two-to-Many Theorem) The scheme (Gen, Enc, Dec) is *perfectly secure* if and only if

  $$Pr[Eve(Enc_k(x_0)) = x_0] \leq 1/2.$$

  Proof.

- **Theorem 1.8** (Two-to-Many Theorem) The scheme (Gen, Enc, Dec) is *perfectly secure* if and only if

  $$Pr[Eve(Enc_k(x_0)) = x_0] \leq 1/2.$$

  Proof.
  The "only if" part is easy (by definition, this is the special case that $|M| = 2$).

  The "if" part is tricky.

- **Theorem 1.8** (Two-to-Many Theorem) The scheme (Gen, Enc, Dec) is *perfectly secure* if and only if

$$Pr[Eve(Enc_k(x_0)) = x_0] \leq 1/2.$$

Proof.

The "only if" part is easy (by definition, this is the special case that $|M| = 2$).

The "if" part is tricky.

We need to show that if there is some set M and some strategy for Eve to guess a plaintext chosen from M with probability larger than $1/|M|$, then there is also some set M' of size 2 and a strategy Eve' for Eve to guess a plaintext chosen from M' with probability larger than $1/2$.

We fix $x_0 = 0^\ell$ and pick x_1 at random in M. Then it holds that for random key k and message $x_1 \in M$,

$$\Pr_{k \leftarrow \{0,1\}^n, x_1 \leftarrow M}[Eve(Enc_k(x_1)) = x_1] > 1/|M|.$$

On the other hand, for every choice of k, $x' = Eve(Enc_k(x_0))$ is a fixed string independent on the choice of x_1, and so if we pick x_1 at random in M, then the probability that $x_1 = x'$ is at most $1/|M|$, i.e.,

$$\Pr_{k \leftarrow \{0,1\}^n, x_1 \leftarrow M}[Eve(Enc_k(x_0)) = x_1] \leq 1/|M|.$$

Due to the linearity of expection,there exists some x_1 satisfying

$$\Pr[Eve(Enc_k(x_1)) = x_1] > \Pr[Eve(Enc_k(x_0)) = x_1]. \text{ (why?)}$$

We now define a new attacker Eve' as: $Eve'(c) = \begin{cases} x_1, & \text{if } Eve(c) = x_1 \\ x_i, i \in \{0,1\} \text{ at random}, & \text{otherwise} \end{cases}$

This means the probability that $Eve'(Enc_k(x_b)) = x_b$ is larger than $1/2$ (Why?).

One-time Pad

- The *XOR* operation: $a \oplus b = a + b \bmod 2$.

One-time Pad

- The *XOR* operation: $a \oplus b = a + b \bmod 2$.

$$a \oplus 0 = a$$
$$a \oplus a = 0$$
$$a \oplus b = b \oplus a \text{ (Commutativity)}$$
$$a \oplus (b \oplus c) = (a \oplus b) \oplus c \text{ (Associativity)}$$

One-time Pad

- The *XOR* operation: $a \oplus b = a + b \bmod 2$.

$$a \oplus 0 = a$$
$$a \oplus a = 0$$
$$a \oplus b = b \oplus a \text{ (Commutativity)}$$
$$a \oplus (b \oplus c) = (a \oplus b) \oplus c \text{ (Associativity)}$$

The One-time Pad scheme (Vernam 1917, Shannon 1949):
$n = |k| = |x|$, $Enc : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$
$Enc_k(x) = x \oplus k$
$Dec_k(y) = y \oplus k$

One-time Pad

- The *XOR* operation: $a \oplus b = a + b \bmod 2$.

$$a \oplus 0 = a$$
$$a \oplus a = 0$$
$$a \oplus b = b \oplus a \text{ (Commutativity)}$$
$$a \oplus (b \oplus c) = (a \oplus b) \oplus c \text{ (Associativity)}$$

The One-time Pad scheme (Vernam 1917, Shannon 1949):
$n = |k| = |x|$, $Enc : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$
$Enc_k(x) = x \oplus k$
$Dec_k(y) = y \oplus k$

Validity:
$$Dec_k(Enc_k(x)) = (x \oplus k) \oplus k = x \oplus (k \oplus k) = x \oplus 0^n = x$$

One-time Pad

- **Theorem 1.9** One-time pad is *perfectly secure*.

One-time Pad

- **Theorem 1.9** One-time pad is *perfectly secure*.

  Proof. Prove that for every $x \in \{0,1\}^n$, the distribution $Y_x = Enc_{U_n}(x)$ is uniformly distributed.

One-time Pad

- **Theorem 1.9** One-time pad is *perfectly secure*.

  Proof. Prove that for every $x \in \{0,1\}^n$, the distribution $Y_x = Enc_{U_n}(x)$ is uniformly distributed.

  Let $y \in \{0,1\}^n$, we need to show that
  $Pr_{k \leftarrow_R \{0,1\}^n}[x \oplus k = y] = 2^{-n}$
  Since there is a unique single value of $k = x \oplus y$, the probability that the equation is true is 2^{-n}.

One-time Pad

- $\mathcal{Q}$: Is this the end of cryptography?

One-time Pad

- $\mathcal{Q}$: Is this the end of cryptography?

  We need more:

  ◇ Use the same key for many plaintexts

  ◇ Use n-bit key for $2n$-bit plaintexts.

One-time Pad

- $\mathcal{Q}$: Is this the end of cryptography?

  We need more:

  ◇ Use the same key for many plaintexts

  ◇ Use n-bit key for $2n$-bit plaintexts.

  Theorem 1.10 (Limitations of perfect secrecy) There is no *perfectly secure* encryption schemes (Gen, Enc, Dec) with n-bit plaintexts and $(n-1)$-bit keys.

One-time Pad

- $\mathcal{Q}$: Is this the end of cryptography?

  We need more:
  - ◇ Use the same key for many plaintexts
  - ◇ Use n-bit key for $2n$-bit plaintexts.

  Theorem 1.10 (Limitations of perfect secrecy) There is no *perfectly secure* encryption schemes (Gen, Enc, Dec) with n-bit plaintexts and $(n-1)$-bit keys.

  Proof.

One-time Pad

- $\mathcal{Q}$: Is this the end of cryptography?

  We need more:

  ⋄ Use the same key for many plaintexts

  ⋄ Use n-bit key for $2n$-bit plaintexts.

  Theorem 1.10 (Limitations of perfect secrecy) There is no *perfectly secure* encryption schemes (Gen, Enc, Dec) with n-bit plaintexts and $(n-1)$-bit keys.

  Proof.

  Suppose that (Gen, Enc, Dec) is such an encryption scheme. Denote by Y_0 the distribution $E_{U_{n-1}}(0^n)$ and by S_0 its support. Since there are only 2^{n-1} possible keys, we have $|S_0| \leq 2^{n-1}$.
  Now for every key k the function $Enc_k(\cdot)$ is one-to-one and hence its image is of size $\geq 2^n$. This means that for every k, there exists x such that $Enc_k(x) \notin S_0$. Fix such a k and x, then the distribution $Enc_{U_{n-1}}(x)$ does not have the same support as Y_0 and hence it is not identical to Y_0.

Next Lecture

- computational security ...