187 - Day 16

Wednesday, May 9, 2018 9:42 AM

. Midterm 2 is this Friday 5/11 during class time
↳ a page of notes (both sides) + calculator.
(review how to compute $\log_2(x)$ on calculator)

. Office hour tomorrow APM 5824 from 4:30 pm – 6pm.

Day 16 – Random Cryptosystem and Perfect Secrecy

Random Crypto-systems

The set up of cryptography

- Message/plaintext space $\mathcal{M} = \{m_1, m_2, \dots, m_N\}$
- Key space $\mathcal{K} = \{k_1, k_2, \dots, k_S\}$
- Ciphertext space $\mathcal{C} = \{c_1, c_2, \dots, c_Q\}$
- The encrypting function corresponding to the key k: $c = E_k(m)$
- The decrypting function corresponding to the key k: $m = D_k(c)$

$$\begin{tikzcd} & m_i \in \mathcal{M} \arrow[dr] & \\ \boxed{D_{k_s}(c_j)} \arrow[ur] & & \boxed{E_{k_i}(m_i)} \arrow[dl] \\ & c_j \in \mathcal{C} \arrow[ul] & \end{tikzcd}$$

k_i may or may not be the same as k_s.

In a random crypto-system:

random variable:
- $M \in \mathcal{M}$ is the chosen message $\quad \mathbb{P}(M = m_i) = p_i$
- $K \in \mathcal{K}$ is the chosen key $\quad \mathbb{P}(K = k_s) = q_s$
- $C \in \mathcal{C}$ is the resulting ciphertext

Remarks:

- We choose the key K independently of the message M. → K & M are independent R.V.
  $\mathbb{P}(M = m_i \cap K = k_s) = \mathbb{P}(M = m_i) \cdot \mathbb{P}(K = k_s)$ for all $m_i \in \mathcal{M}$, $k_s \in \mathcal{K}$
- $C = E_K(M)$ so the ciphertext C is a random variable which depends on M and K.
- $M = D_K(C)$ so $\boxed{H(K, C) = H(K, M)}$ ✓
  If your enemy knows K and C ↓ your enemy will know M
- $H(K|C)$ is the remaining uncertainty about the key after we intercept the ciphertext.

$$H(K|C) = 0 \Leftrightarrow \text{the ciphertext determines the key}$$

↓ your enemy loves this ; You don't want.

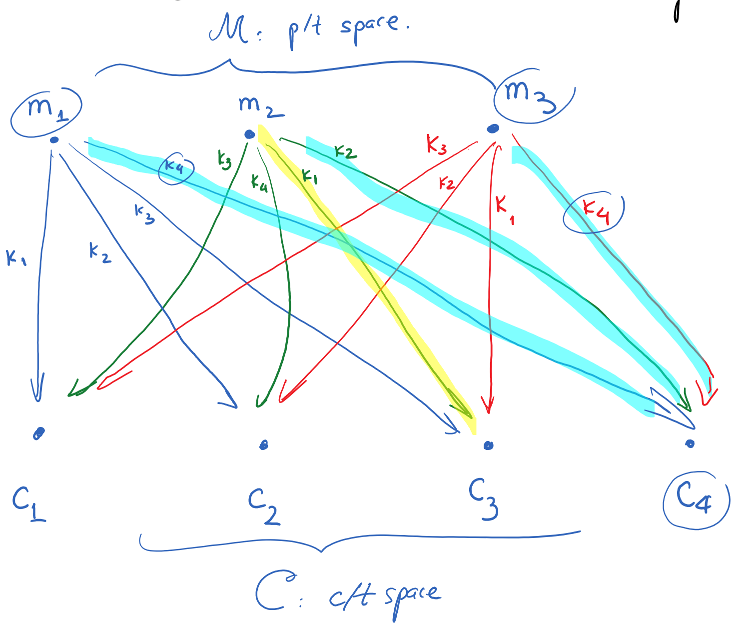
1

3 messages m_1, m_2, m_3

4 keys, 4 ciphertexts

Example.

4 keys



randomize

If $M = m_2$, $K = k_1$ then $C = c_3$

When enemy sees C_4. there are 3 cases:

- $M = m_1$, $K = k_4$
- $M = m_2$, $K = k_2$
- $M = m_3$, $K = k_4$

Theorem 1. *For* ***ciphertext only*** *attack:*

$$H(K|C) = H(K) + H(M) - H(C)$$

The remaining uncertainty your enemy has about the key, given that they know the ciphertext.

proof: Key and plaintext are independent.

So $H(K,M) = H(K) + H(M)$

Also, $H(K,C) = H(K,M) = H(K) + H(M)$

But $H(K,C) = H(C) + H(K|C)$

(Day 13)

$H(C) + H(K|C) = H(K) + H(M)$.

So $H(K|C) = H(K) + H(M) - H(C)$

the enemy knows C and M

a part of the p/text.

Theorem 2. *For* ***known plaintext*** *attack:*

$$H(K|C,M) = H(K) - H(C|M)$$

remaining uncertainty about the key after knowing C and M.

proof: $H(K,C,M) \underset{\text{Day 13}}{=} H(K|C,M) + H(C,M)$

. $C = E_K(M) \Rightarrow H(K,C,M) = H(K,M)$

So $H(K,M) = H(K,C,M) = H(K|C,M) + H(C,M)$

. K & M are indep. $\Rightarrow$

$H(K,M) = H(K) + H(M) = H(K|C,M) + H(C,M)$

$\Rightarrow H(K) + \cancel{H(M)} = H(K|C,M) + H(C|M) + \cancel{H(M)}$

$\Rightarrow H(K|C,M) = H(K) - H(C|M)$

in order to figure out the key from C and a portion of the plaintext = uncertainty about the key − amount of info I get from knowing ciphertext, given that I know parts of the plaintext.

Definition 1. *A cryptosystem is said oi attain* ***perfect secrecy*** *if the* ***ciphertext gives no information about the plaintext****. That is, M, C are random variable, namely,*

$$\mathbb{P}(M = m_i \cap C = c_j) = \mathbb{P}(M = m_i) \cdot \mathbb{P}(C = c_j)$$

for all $m_j \in \mathcal{M}$ and $c_j \in \mathcal{C}$.

In a perfect secrecy system

- Thus the number of keys must be at least as large as the number of ciphertexts.
- For a fixed key: different plaintexts must go to different ciphertexts. Thus, the number of ciphertexts must be at least as large as the number of plaintexts.

$\boxed{\# \text{ keys} \geq \# \text{ ciphertext} \geq \# \text{ plaintext}}$.

guarantee at least a 1-1 mapping b/w C and M.

$\mathbb{P}(M = m_2 \cap C = c_1) = ?$

$c_1 = \mathbb{P}(M = m_2, K = k_3)$

$= \mathbb{P}(M = m_2) \cdot \mathbb{P}(K = k_3)$

$= m_2 \cdot \frac{1}{4} = \mathbb{P}(M = m_2) \cdot \mathbb{P}(C = c_1)$

* You can then check that for any

guarantee at least a 1-1 mapping b/w C and M.

Q: Does the system on P.2 have perfect secrecy?

. Suppose $\begin{cases} \mathbb{P}(M=m_1)=p_1, \ \mathbb{P}(M=m_2)=p_2, \ \mathbb{P}(M=m_3)=p_3 \\ \mathbb{P}(K=k_i)=1/4 \quad \text{for any key } k_i \end{cases}$

$$\mathbb{P}(C=c_1)= \mathbb{P}(m_1,k_1)+\mathbb{P}(m_2,k_3)+\mathbb{P}(m_3,k_3)$$
$$= \mathbb{P}(m_1)\mathbb{P}(k_1)+\mathbb{P}(m_2)\mathbb{P}(k_3)+\mathbb{P}(m_3)\mathbb{P}(k_3)$$
$$= p_1\cdot\frac{1}{4}+p_2\cdot\frac{1}{4}+p_3\cdot\frac{1}{4} = \frac{1}{4}.$$

Similarly, $\mathbb{P}(C=c_2)=\mathbb{P}(C=c_3)=\mathbb{P}(C=c_4)=\frac{1}{4}$.

* You can then check that for any pair (m_i, c_j), we always have
$$\mathbb{P}(M=m_i \cap C=c_j)=p_i\cdot\frac{1}{4}$$
$$=\mathbb{P}(M=m_i)\cdot\mathbb{P}(C=c_j)$$

So M, C are indep. $\Rightarrow$ system has perfect secrecy.

5

Theorem 3. *Perfect secrecy is achieved when*

- *All keys are equally likely* $\longrightarrow$ to maximize $H(K)$
- *For each pair (m_i, c_j) there is a* ***unique*** *key k_s such that $E_{k_s}(m_i)=c_j$*

↳ (There's ONLY one way to encrypt $m_i \to c_j$)

proof: For any pair $(M,C)=(m_i,c_j)$

$$\mathbb{P}(C=c_j)=\sum_i \underbrace{\mathbb{P}(M=m_i)}_{\text{(all pos. p/t)}}\cdot\underbrace{\sum_{E_{k_s}(m_i)=c_j}\mathbb{P}(K=k_s)}_{\text{(all pos. ways that } m_i\to c_j)}.$$

. Since there's only one key k_s that can encrypt $m_i \to c_j$

and $\mathbb{P}(K=k_s)=1/|K|$ (all keys are equally likely)

Then $\mathbb{P}(C=c_j)=\sum_i \underbrace{\mathbb{P}(M=m_i)}_{1}\cdot\frac{1}{|K|}=\frac{1}{|K|}.$

$$\mathbb{P}(M=m_i \cap C=c_j)=\sum_{E_{k_s}(m_i)=c_j}\mathbb{P}(M=m_i).\mathbb{P}(K=k_s)=\mathbb{P}(M=m_i).\frac{1}{|K|}$$
$$=\mathbb{P}(M=m_i).\mathbb{P}(C=c_j)$$

These calculations are similar to the example above.

6

How to construct a cryptosystem with perfect secrecy?

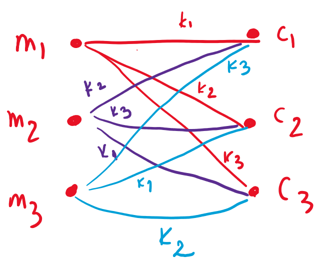
A simplest system w/ perfect secrecy will have:

- # keys = # plaintexts = # ciphertexts.
- All keys are equally likely.
  $\mathbb{P}(K = k_i) = 1/|K|$
- Encryption scheme is a Latin Square or equiv. the encryption diagram has a perfect matching.

Latin Square : Sudoku

	m_1	m_2	m_3
k_1	c_1	c_3	c_2
k_2	c_2	c_1	c_3
k_3	c_3	c_2	c_1

$\Longleftrightarrow$



Definition 2. *A one time pad cryptosystem is a system in which we encrypt a message of length N using N* ***random integer keys*** *$k_1, k_2, \ldots, k_N$.*

The vector $(k_1, k_2, \ldots, k_N)$ is called the ***key stream****.*

Theorem 4. *The one time pad system achieves perfect secrecy.*