ELE 538 - Information Theoretic Security

Instructor: Paul Cuff

Term: 2016 - 2017 Fall

Simple Substitution

September 15, 2016
Thursday

a → d
b → e
c → f
⋮

Julius Caesar

Augustus Caesar

Shift: Key $K \in \{1, 2, \ldots, 26\}$

Simple: Key $K \in [26!]$ → $\approx 2^{88}$ bit but still not too secure

Message: MONKEY ... ← Cyclic Shift Sub Cipher

Key: $\oplus$ k k k k k k

Ciphertext: M⊕k, O⊕k, ...

ex → PRQNHB
k=3 ↗

Message: $M_1 M_2 M_3 M_4 \ldots$ ← vernam cipher

$\oplus k_1 k_2 k_3 k_4 \ldots$ Change the key

binary XOR

If used twice with same key

$$(M^{(1)} \oplus K) \ominus (M^{(2)} \oplus K) = M^{(1)} \ominus M^{(2)}$$

English ⇝ entropy rate is 1 - 1.5 bits/letter

$\log_2 26 = 4.7$ bits/letter

↳ so it is quite redundant language

One time pad:

Vernam Cipher with uniformly distributed key. (each key symbol is independent and don't reuse)

↳ "Perfect Secrecy"

Perfect Secrecy: Ciphertext W

Message M

Key K

$P_{W|M=m}$ does not depend on m at all ("Eve" cannot decode)

$P_{W|K=k, M=m}$ must depend on m in order for "Bob" to decode.

Perfect Secrecy in one sentence: M independent of W.

But independence is usually reserved for r.v's

$M \perp W$ $P_{MW} = P_M \cdot P_W$, $P_{W|M} = P_W$

One time pad is optimal ✓

(Shannon shows its converse (if perfect secrecy then key size must equal message size)

↳ here is its proof:

$$|K| \geq \max_m |W_m| = |W| \geq |M|$$

- $|K| \geq \max_m |W_m|$: ↓ key set; ↑ Assumption: Encoding is deterministic
- $\max_m |W_m| = |W|$: ↑ due to perfect secrecy assumption; conditioned on the message
- $|W| \geq |M|$: ↓ message set; ↓ cipher text set
- ↳ see exploration on next page

$$|W| \geq \max_k |W_k| \geq \min_k |W_k| \geq |M|$$

due to decodability assumption
(I need to be able to decode from the cipher text with given correct key)

Lastly,

$$|W| \geq \max_k |W_k| \quad \leftarrow W \text{ is union of } W_k$$

$$= \max_k \left| \bigcup_m W_{k,m} \right| \quad \text{def of } W_k$$

$$= \max_k \sum_m |W_{k,m}| \quad \text{decodability } (W_{k,m_1} \text{ and } W_{k,m_2} \text{ must be disjoint})$$

$$= \frac{1}{|K|} \sum_{m,k} |W_{k,m}| \quad \text{avg vs max}$$

$$= \frac{|M|}{|K|} \frac{1}{|M|} \sum_{m,k} |W_{k,m}|$$

$$\geq \frac{|M|}{|K|} \min_m \sum_k |W_{m,k}| \quad \text{avg vs min}$$

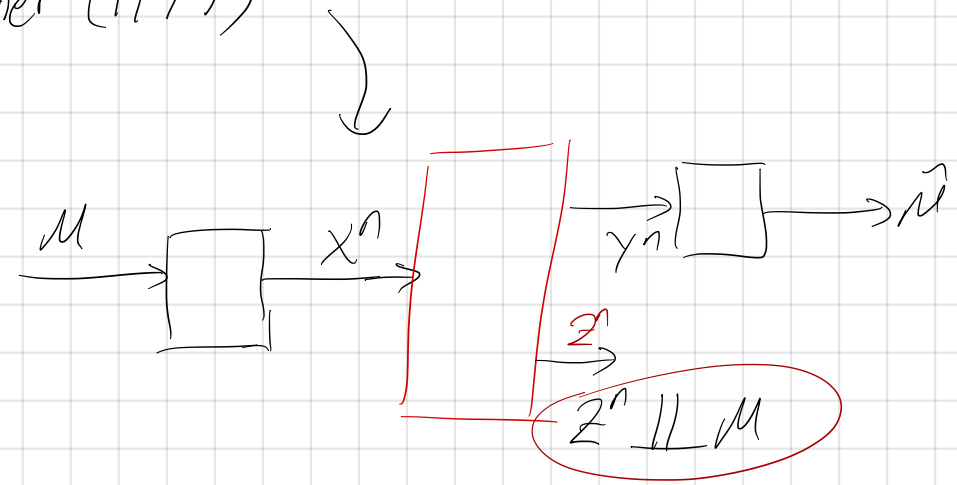
$$\geq \frac{|M|}{|K|} \min_m \left| \bigcup_k W_{m,k} \right| \quad \text{nothing fancy,}$$

$$= \frac{|M|}{|K|} \min_m |W_m| \quad \text{defn of } W_m$$

$$= \frac{|M|}{|K|} |W| \quad \text{due to secrecy assumption } |W_{m_1}| = |W_{m_2}| = |W|$$

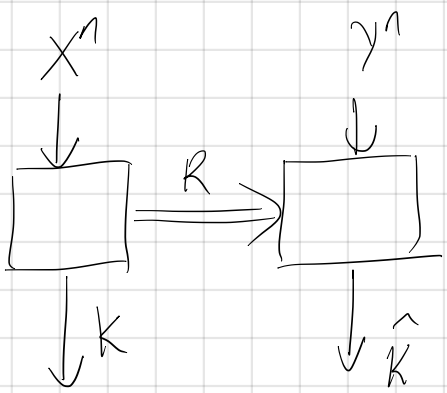
$$\Rightarrow |K| \geq |M| \quad \text{which is the converse}$$

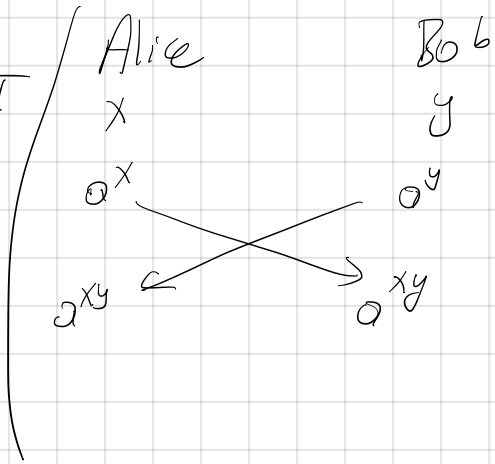
1.) Wyner (1975)



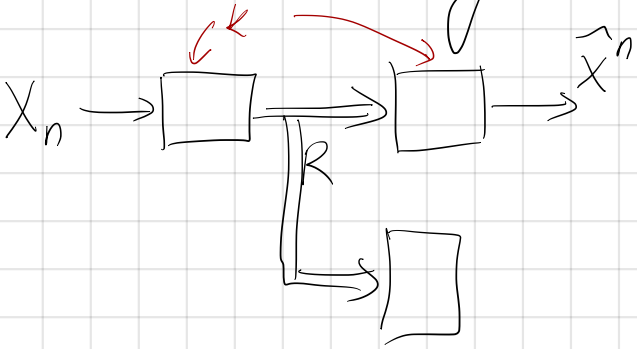
2.) Key Agreement

Diffie-Hellman (1975) on Trans. IT





3.) Secure Source Coding



4) Differential Privacy