

# Perfect Secrecy

Prof. Zeph Grunschlag

## Message Indistinguishability

- Even if narrow possibilities down to two possible plaintexts and have ciphertext, cannot distinguish which plaintext was sent.

DEF2: A cryptosystem  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$  is **perfectly message indistinguishable** if for all plaintexts  $x_1, x_2$  and all ciphertexts  $y$

$$\Pr[e_K(x_1) = y] = \Pr[e_K(x_2) = y]$$

- DEF2 doesn't use random variables  $\mathbf{X}, \mathbf{C}$

# Shannon Secrecy

Knowing ciphertext doesn't help decipher:

- $\mathbf{X}$  - random variable for plaintexts
- $\mathbf{C}$  - random variable for ciphertexts with respect to possible plaintext and keys

DEF1: A cryptosystem  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$  is **Shannon secure** if  $\mathbf{X}$  and  $\mathbf{C}$  are independent. I.e., for all plaintexts  $x$  and ciphertexts  $y$   $\Pr[x|y] = \Pr[x]$ .

- $\mathbf{C}$  depends on implicit rand. var.  $\mathbf{K}$  for keys

## Key Ambiguity

- If any plaintext message could result from a given ciphertext message and all keys equally likely, no knowledge gained about plaintexts.

DEF3: A cryptosystem  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$  with equal size spaces  $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$  is **perfectly key ambiguous** if keys are picked uniformly and for all  $x \in \mathcal{P}, y \in \mathcal{C}$  there is a unique key  $K$  such that  $y = e_K(x)$ .

# One Time Pad

- XOR the plaintext bitstring with key *but* never re-use same key
- Similar to Vigenère but with size of key equaling size of message

DEF: The **one time pad** (OTP) is the cryptosystem defined by  $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n$  and  $e_K(x)_i = x_i \oplus K_i = d_K(x)_i$ , with keys chosen according to uniform distribution.

THM: OTP is perfectly key ambiguous.

5

# Limitations of One Time Pad

- Very large key-size
- **Stateful**: Alice and Bob must keep track of “state” - prone to transmission errors
- Abuse (using twice) results in easily attacked cipher
- Useless for other cryptographic protocols such as authentication

7

# Equivalence of Definitions

- DEF1  $\Leftrightarrow$  DEF2
- If plain-space = cipher-space = key-space:  
DEF1  $\Leftrightarrow$  DEF2  $\Leftrightarrow$  DEF3
- **Perfect secrecy** refers to all definitions

THM: Shannon secrecy and message indistinguishability are equivalent. When restricting to  $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$  key ambiguity is equivalent as well.

LEMMA:  $|\mathcal{K}| < |\mathcal{P}|$  implies *not* perfectly secret.

6

# Other Security Models

- Resistance to all known attacks
- Computational security - cracking would solve impossibly hard problem
  - I. Total break - *recover key*
  - II. Partial break - *can decrypt ciphertexts, without knowing key*
  - III. Semantic break - *can learn a “bit” of information about plaintext, so can distinguish ciphertexts*

8