

Cryptography and Information Theory

Brute Force and Cryptanalysis

Sang-Yoon Chang, Ph.D.

Module Objectives

1. Brute Force Attack
2. Cryptanalysis
3. Perfect Secrecy

Brute Force Attack

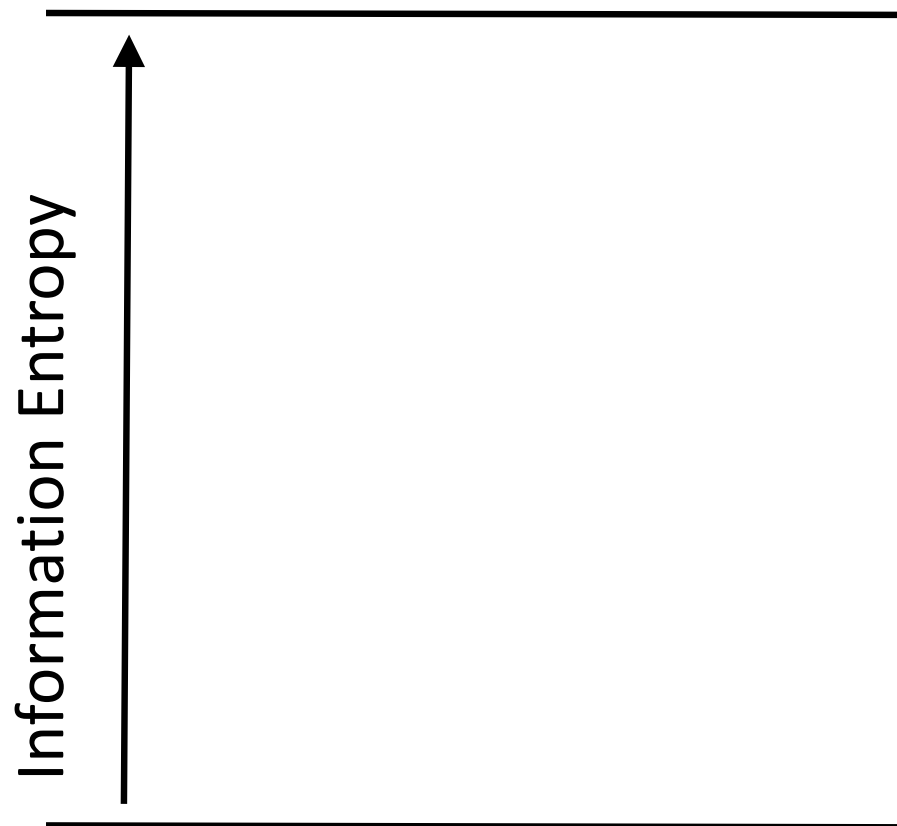


Attacker tries all possible keys until it finds the correct key

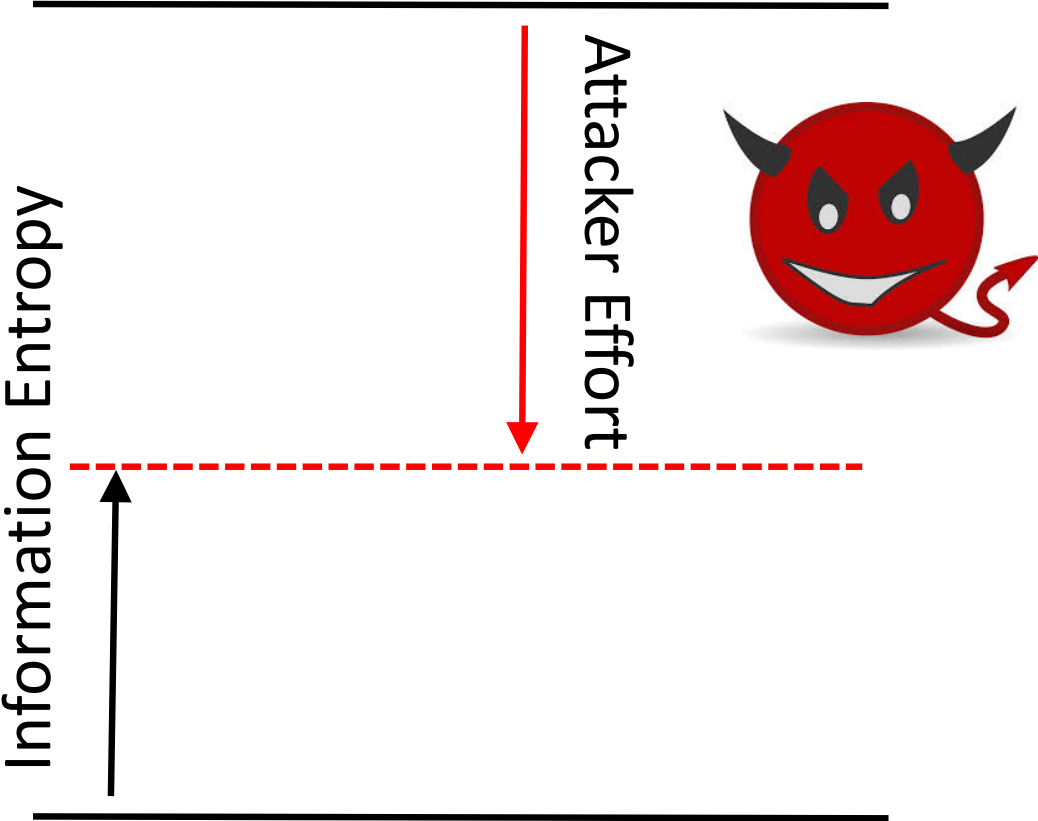
Attacker selects the keys (to try) randomly

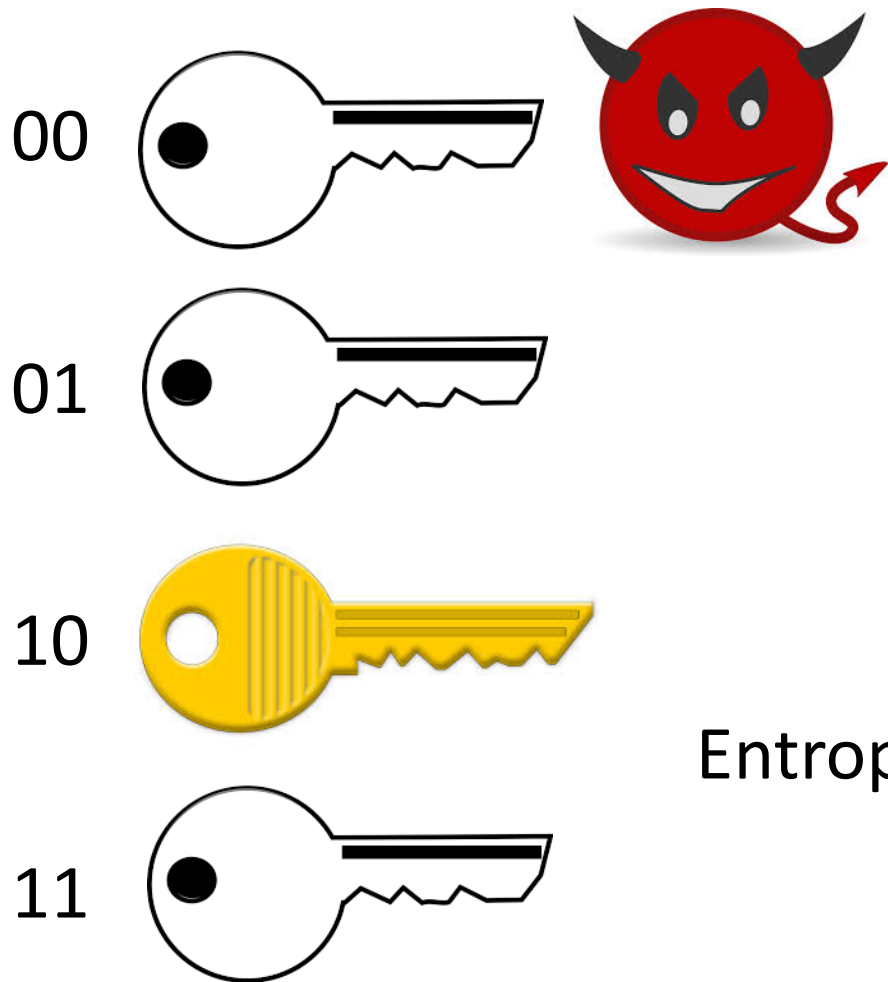
Assume that attacker can distinguish the correct and the incorrect key after trials

Key Strength

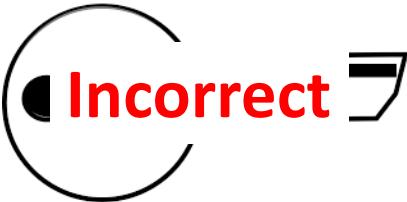


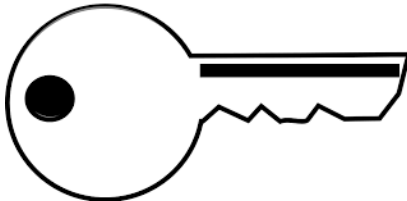
Key Strength



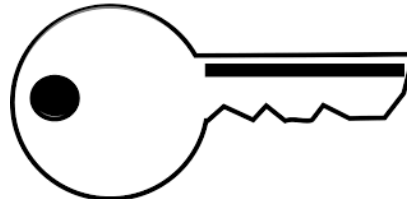


Entropy = 2 bits

00  **Incorrect**

01 

10 

11 



Entropy = $\log_2 3$ bits

Brute Force Attack



With keys that are “n” bits long,
there are 2^n possible keys

Attacker can succeed in the attack
in the 1st try (best case) or the
last try (worst case; 2^n tries)

On average, attacker will try 2^{n-1} tries

Cryptanalysis



Studying and analyzing the cryptosystem in order to effectively decipher the coded message *without* the key

Cryptanalysis



Attacker can know which keys are more likely than others

Use the information to more quickly find the key

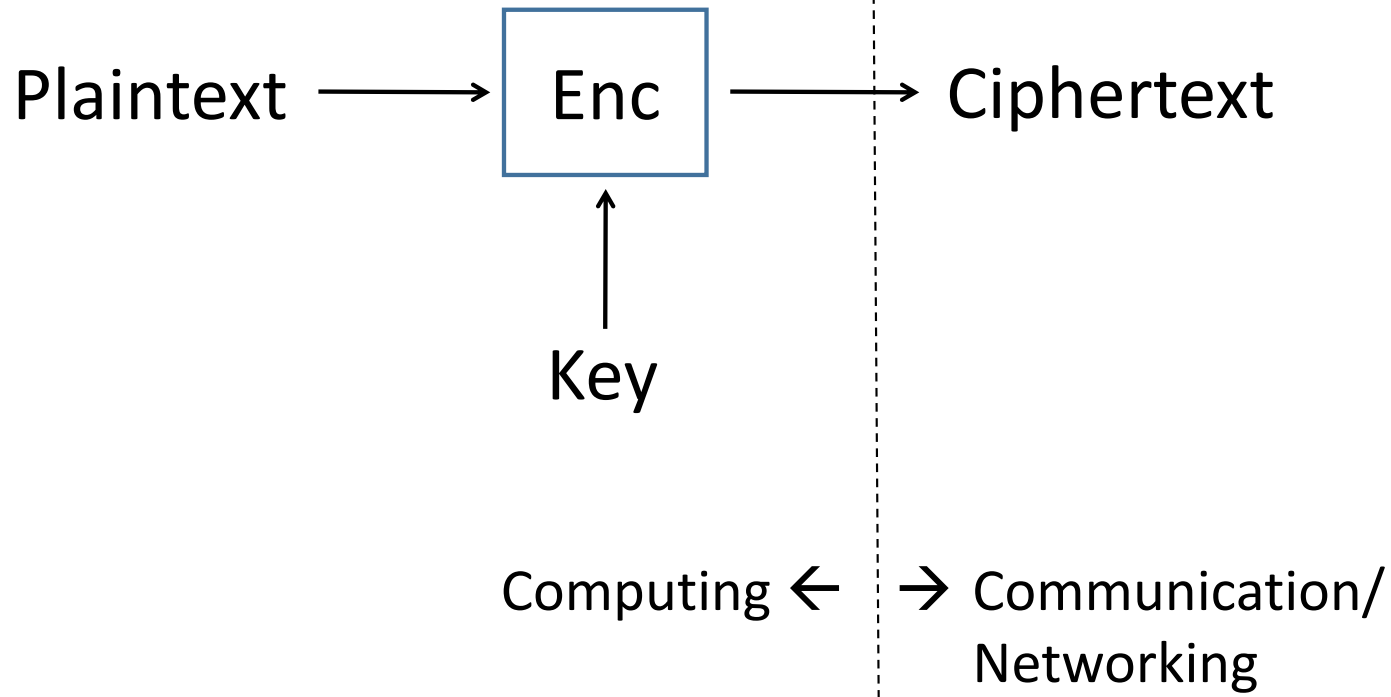
The non-uniform distribution of the key selection yields entropy reduction



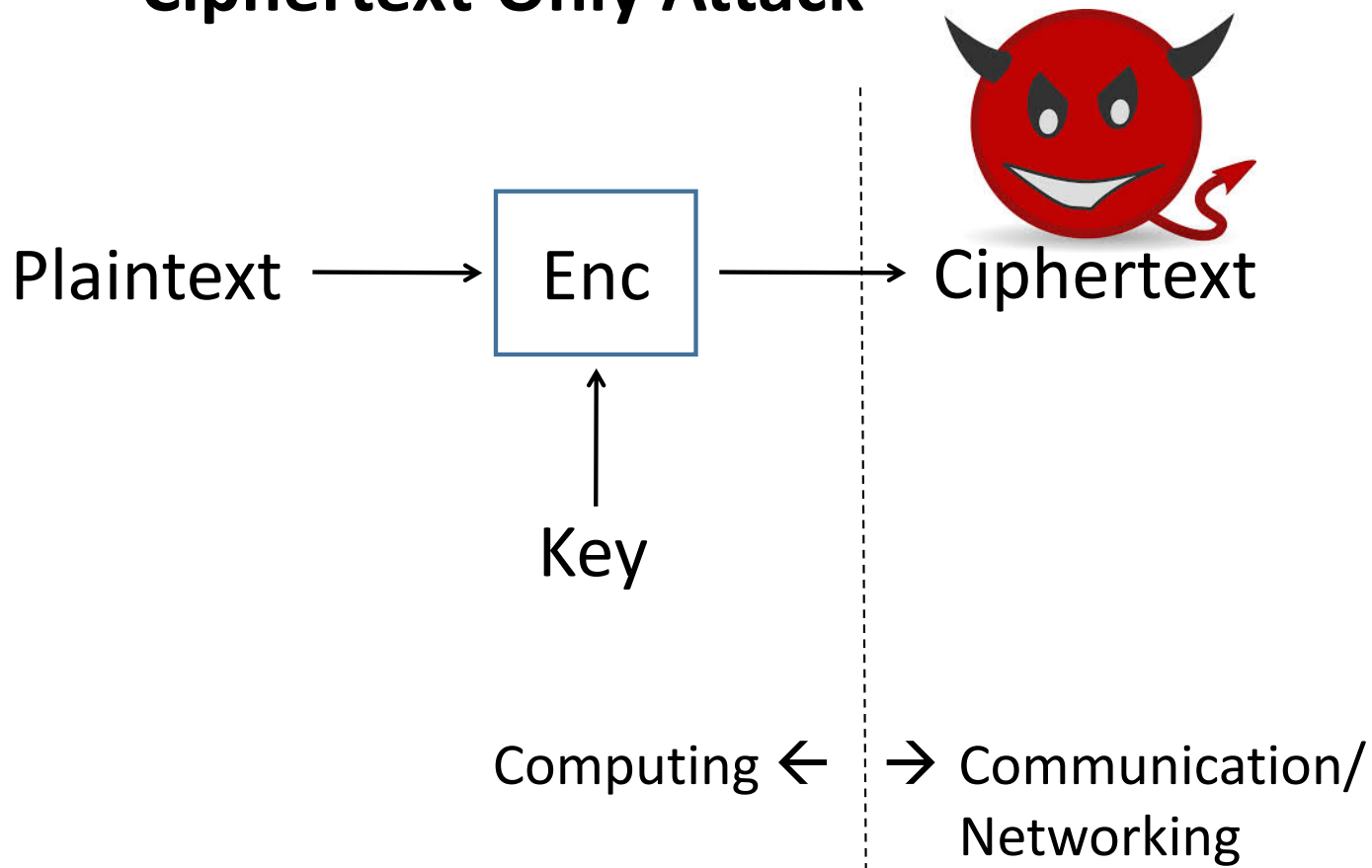




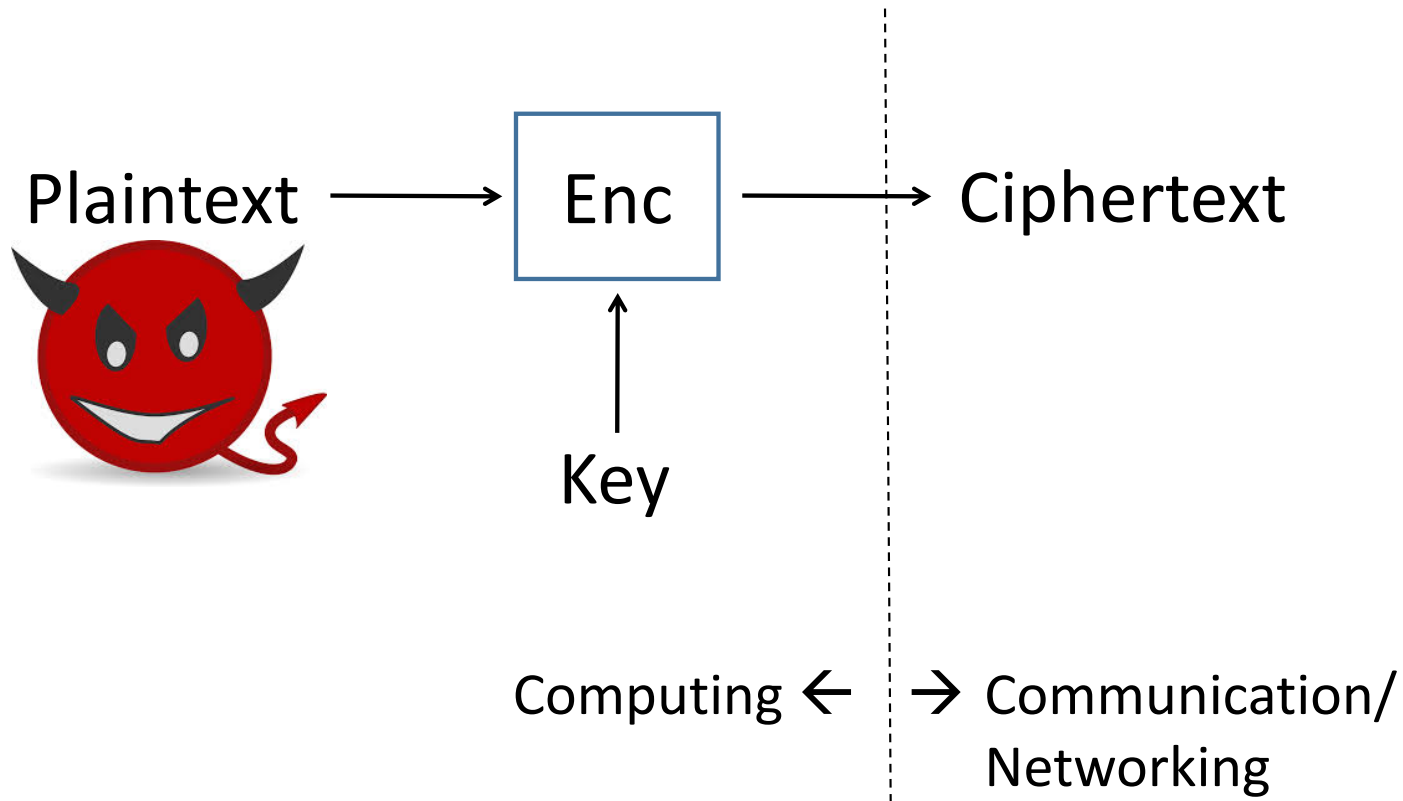
Cryptanalysis



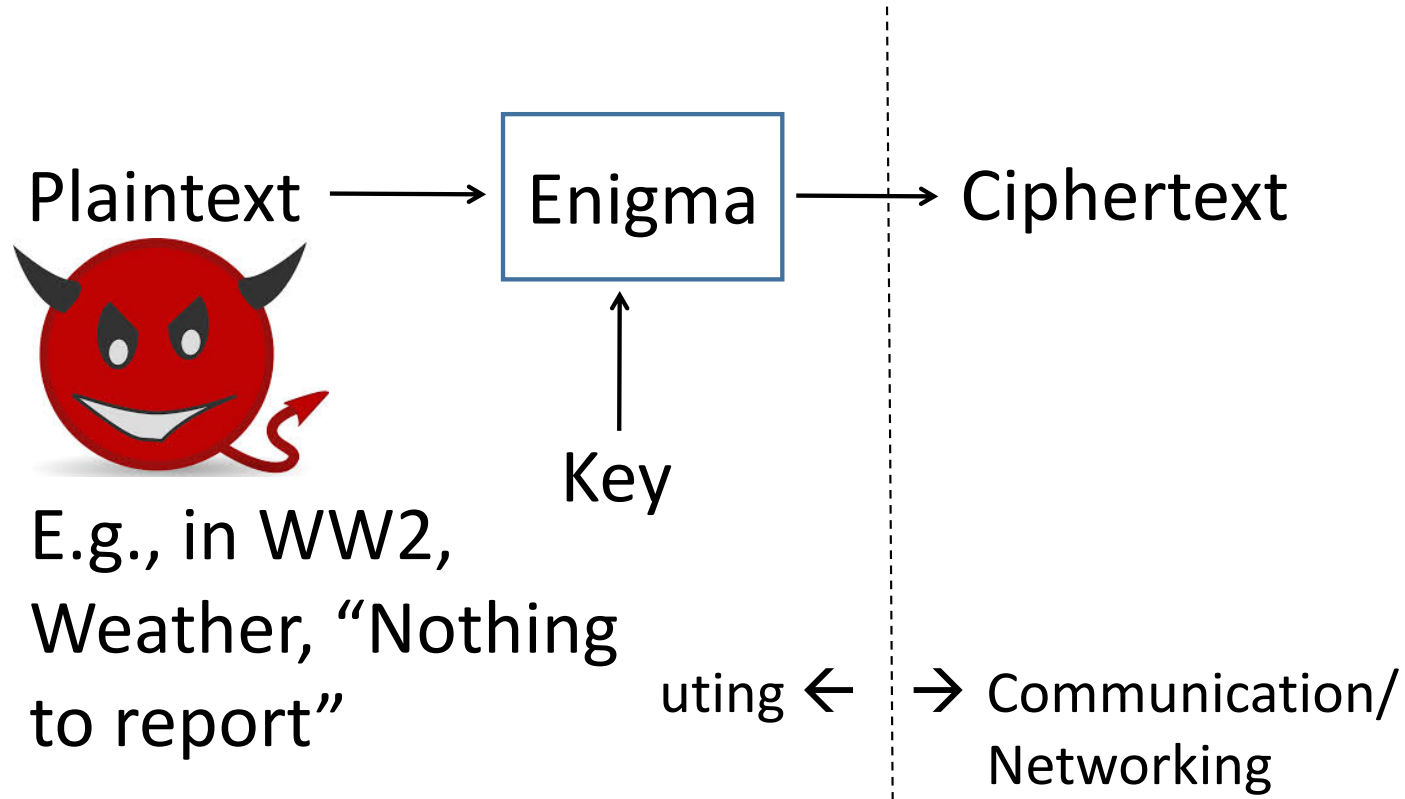
Ciphertext-Only Attack



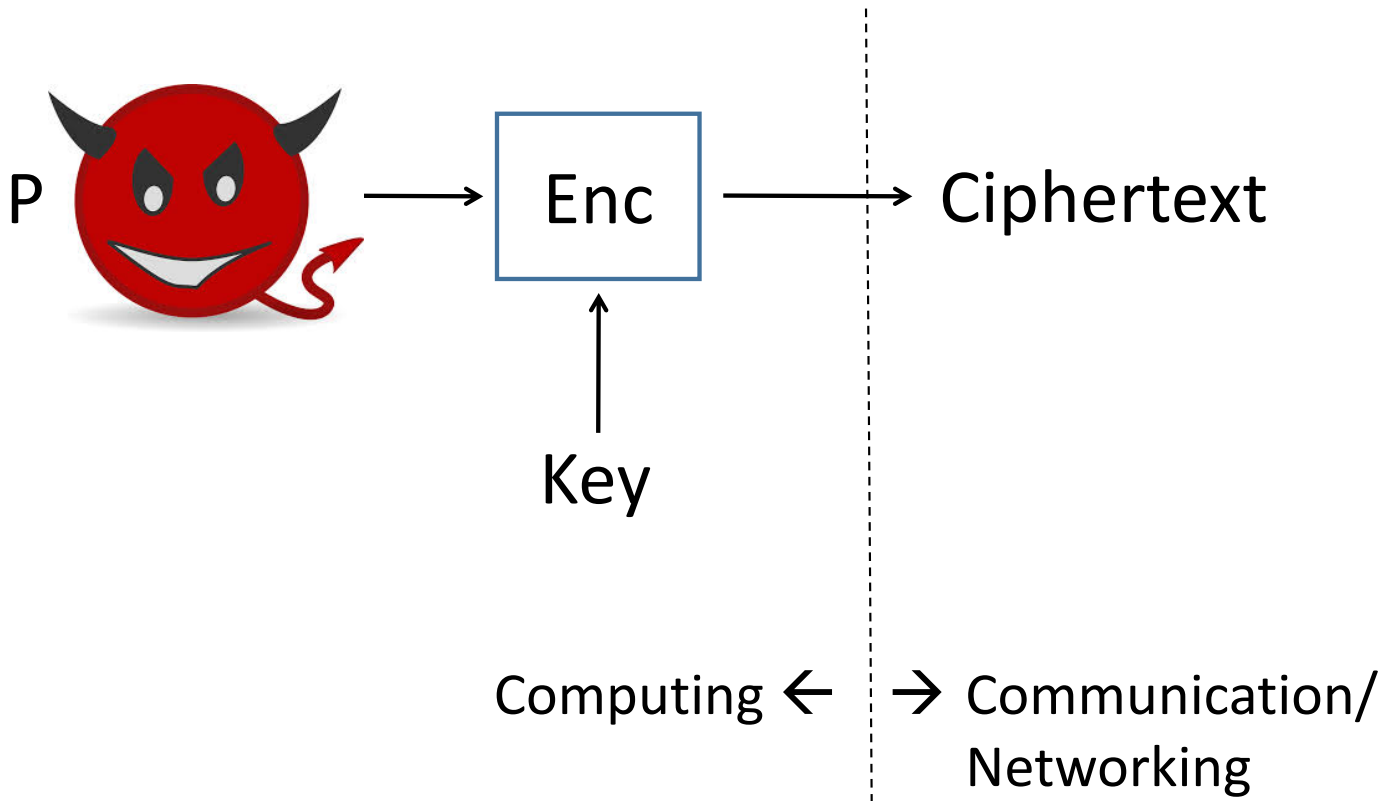
Known-Plaintext Attack



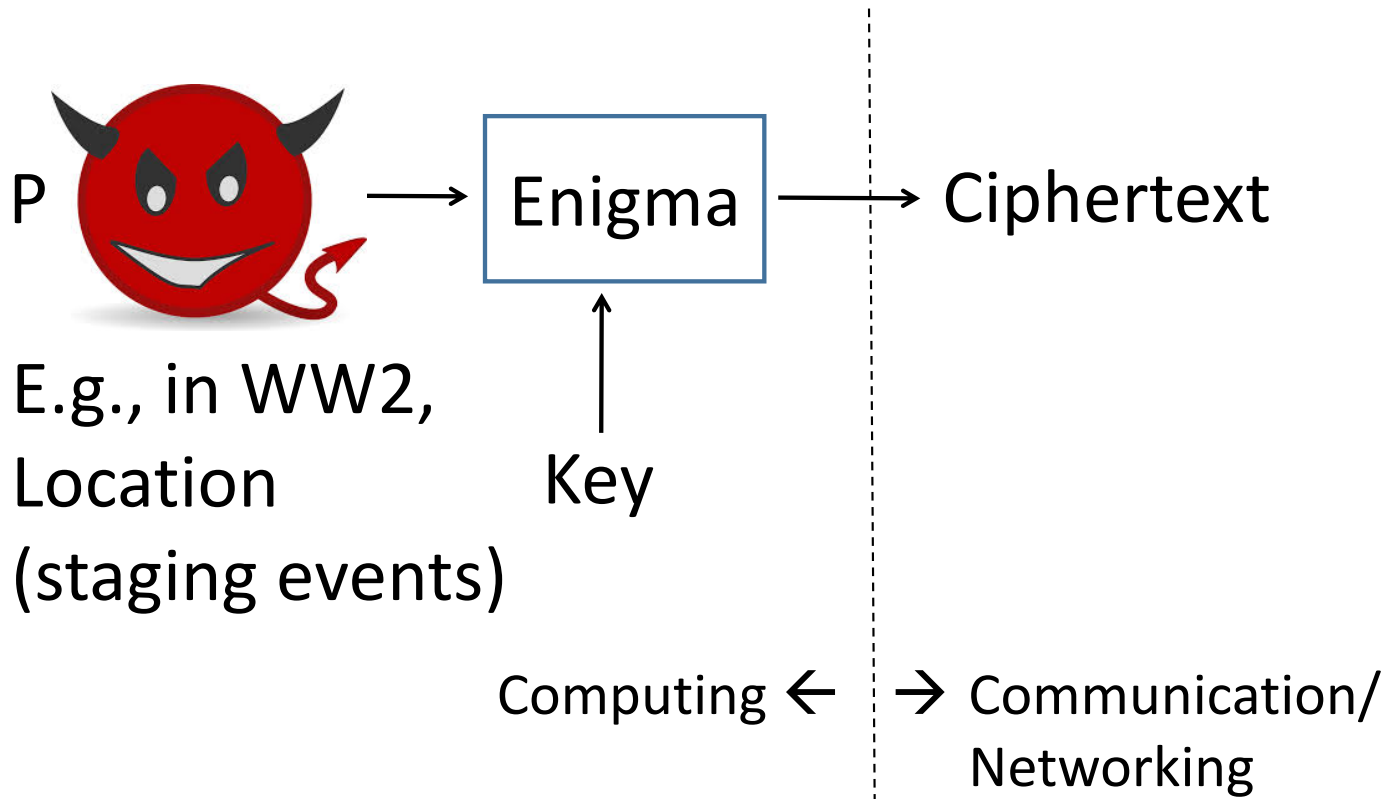
Known-Plaintext Attack



Chosen-Plaintext Attack



Chosen-Plaintext Attack



Perfect Secrecy

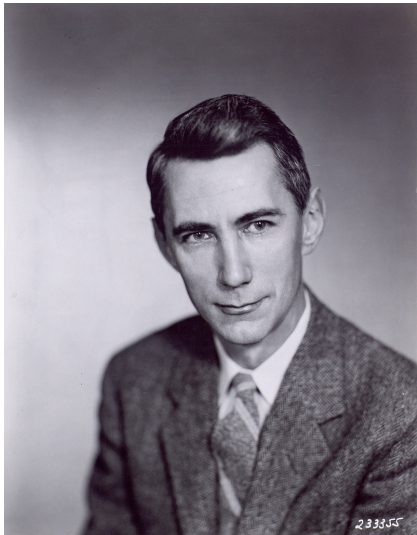
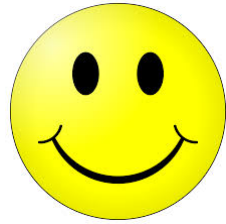


Ciphertext provides no information about the plaintext without the key

Holds regardless of the attacker's computational capabilities

Cryptanalytically unbreakable

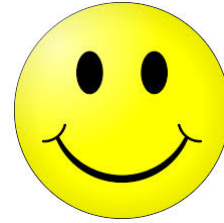
One-Time Pad



The key entropy is as great
as the message entropy,
even as the message grows

Achieves perfect secrecy

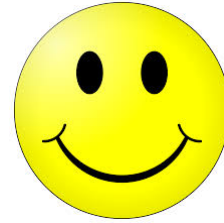
Practicality of One-Time Pad



Two challenges that limit its practicality:

- Key and randomness generation
- Key distribution and agreement

Practicality of One-Time Pad



Two challenges that limit its practicality:

- Key and randomness generation
- Key distribution and agreement

Examples of its use:

- Low-bandwidth applications
(e.g., mission-critical messages)
- Cryptosystem design, e.g., key refresh

