

CIS 4360, SPRING 2026

CRYPTOGRAPHY

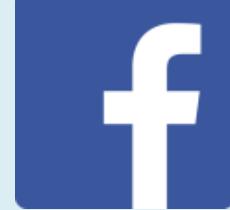
VIET TUNG HOANG

Agenda

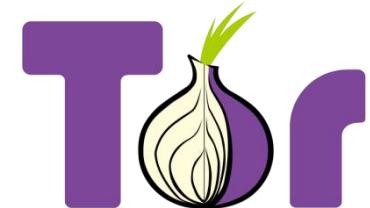
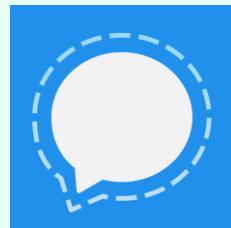
1. Crypto Usage & Goal
2. Classical Crypto
3. One-time Pad & Perfect Secrecy
4. Modern Crypto

Crypto Use Is Ubiquitous

HTTPS



Secure
messaging



Bitcoin

A Classical Crypto Goal: Privacy



Transfer \$5 to
account 12345

K_e



K_d



Privacy: Adversary can't learn anything from the content that it eavesdrops.

A Classical Crypto Goal: Privacy



1100000100101
0101011110111

K_e



K_d



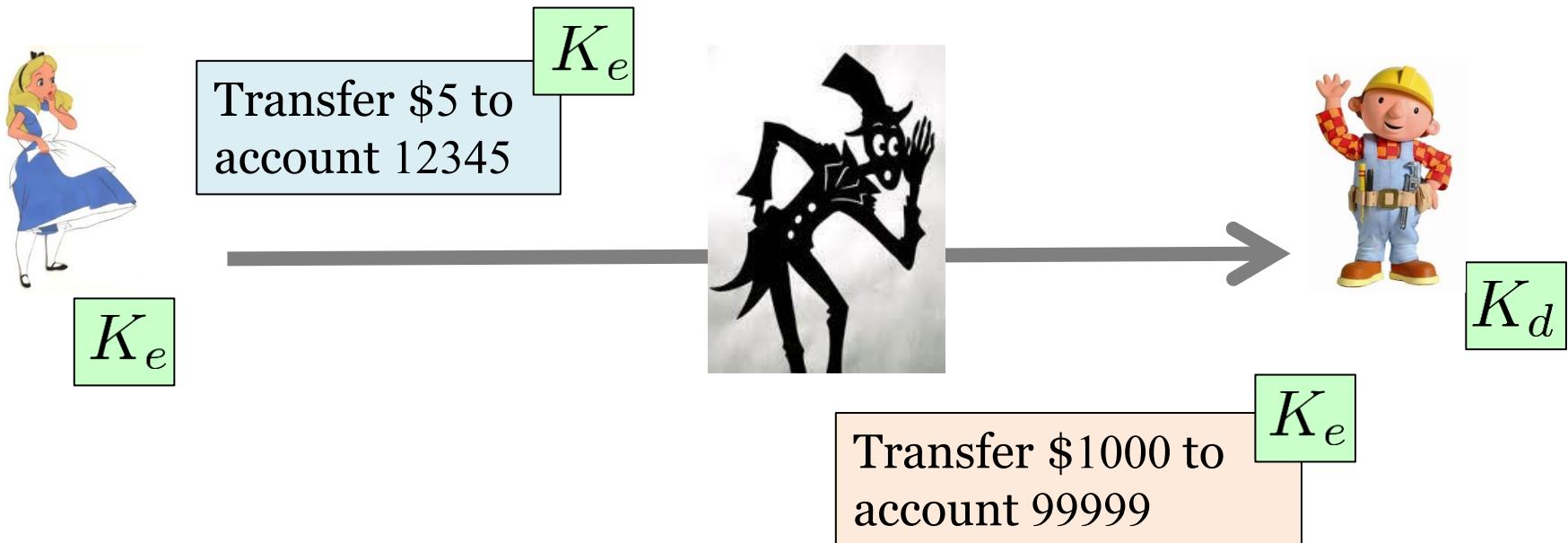
Private-key setting: $K_e = K_d$

secret

Public-key setting: $K_e \neq K_d$

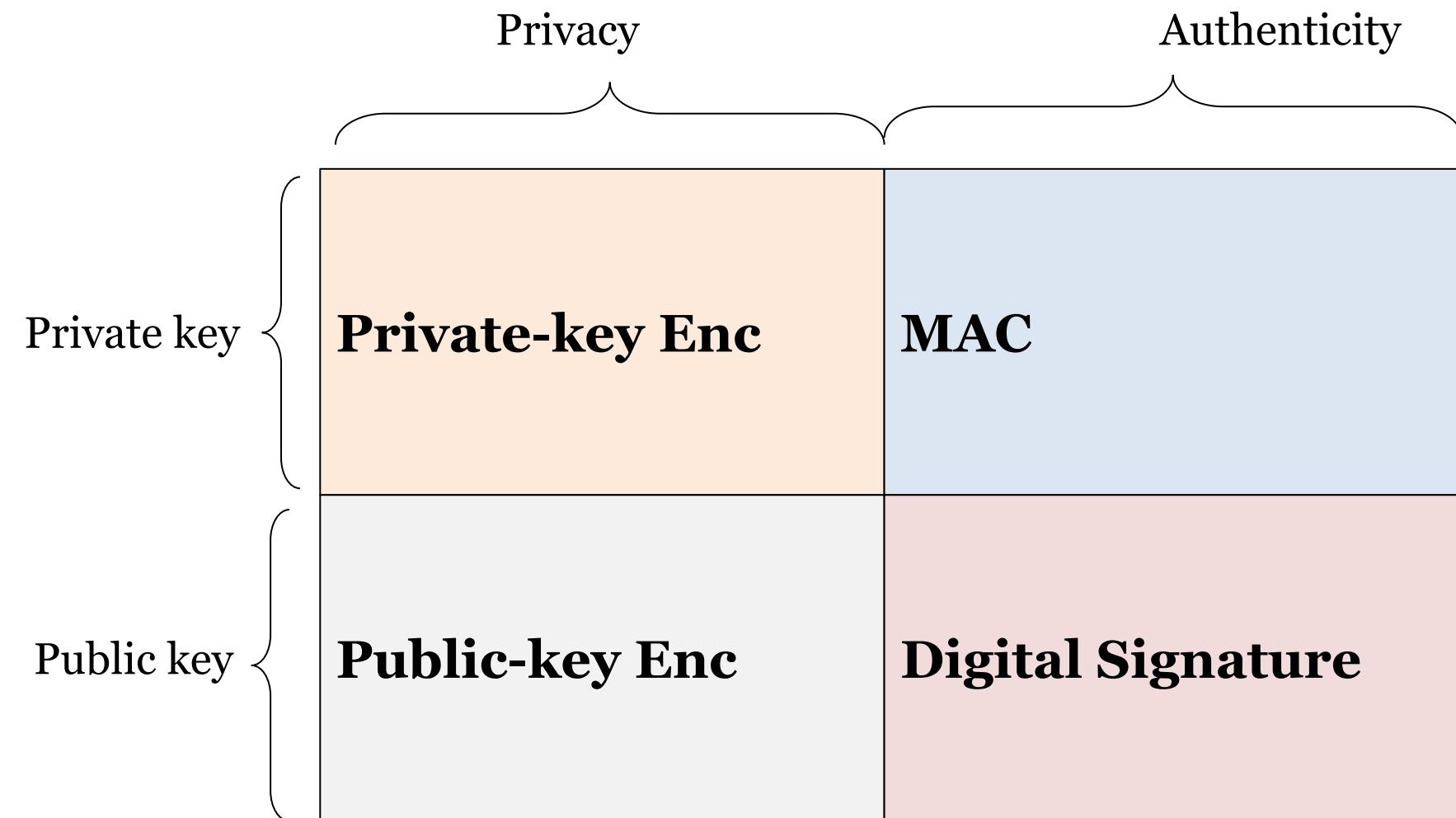
public secret

But Privacy Alone Is Not Enough



Authenticity: Adversary can't forge valid ciphertexts

Four Fundamental Cryptographic Problems



Agenda

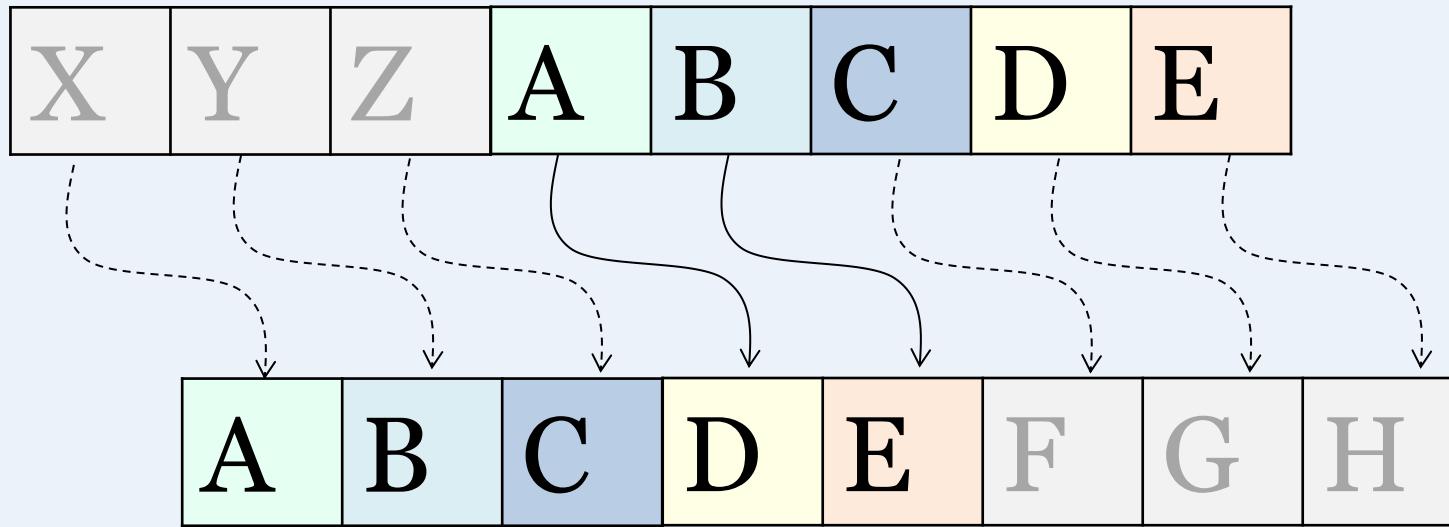
1. Crypto Usage & Goals

2. Classical Crypto

3. One-time Pad & Perfect Secrecy

4. Modern Crypto

Caesar Cipher



No key

Broken once scheme is known

Caesar Cipher In The Wild



This article is more than 1 year old

Mafia boss undone by clumsy crypto

Little Caesar

 [John Leyden](#)

Wed 19 Apr 2006 // 14:14 UTC

Clues left in the clumsily encrypted notes of a Mafia don have helped Italian investigators to track his associates and ultimately contributed to his capture after years on the run.



This article is more than 1 year old

BA jihadist relied on Jesus-era encryption

30 years for airline bomb plot

 [Team Register](#)

Tue 22 Mar 2011 // 11:52 UTC

An IT worker from British Airways jailed for 30 years for terrorism offences used encryption techniques that pre-date the birth of Jesus.

Shift Cipher

Use a secret key $K \in \{0, \dots, 25\}$

Same as Caesar cipher, but shift K positions, instead of 3.

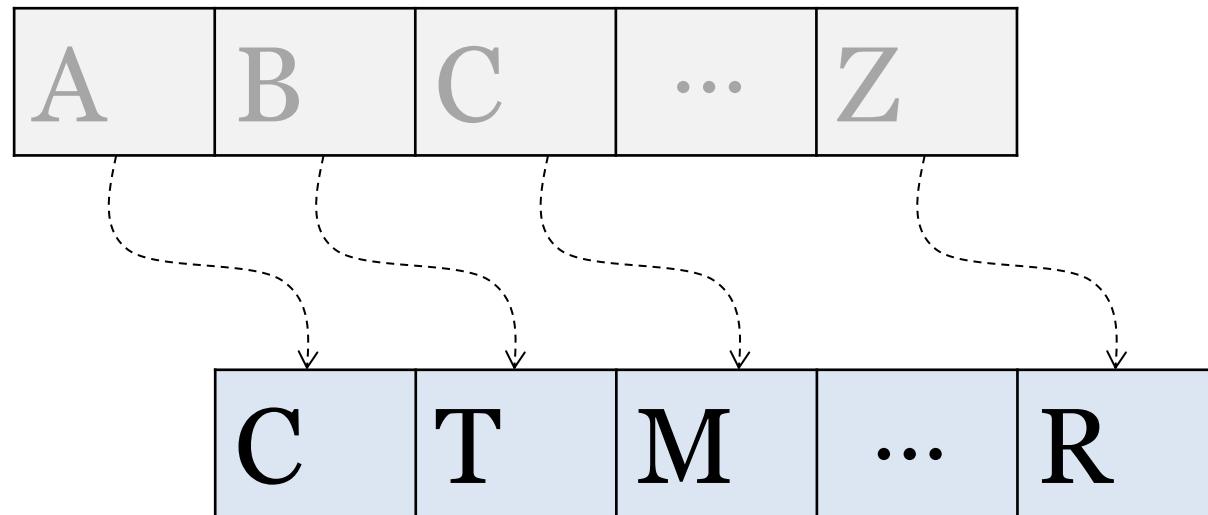


**Small Keyspace
Broken by brute force**

Substitution Cipher

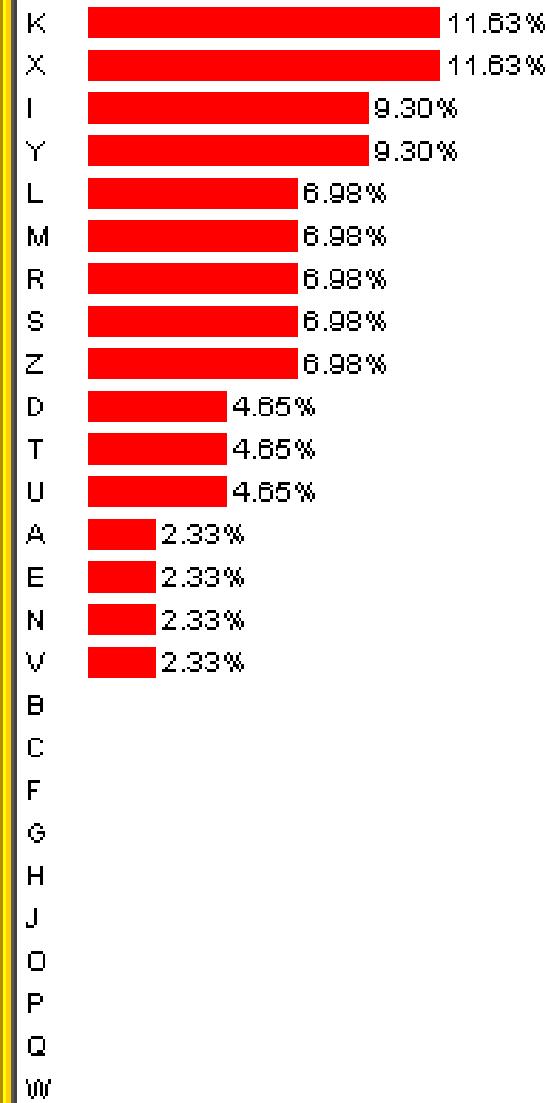
Key: a permutation $\pi : \Sigma \rightarrow \Sigma$

Example: $\Sigma = \{A, B, C, \dots, Z\}$

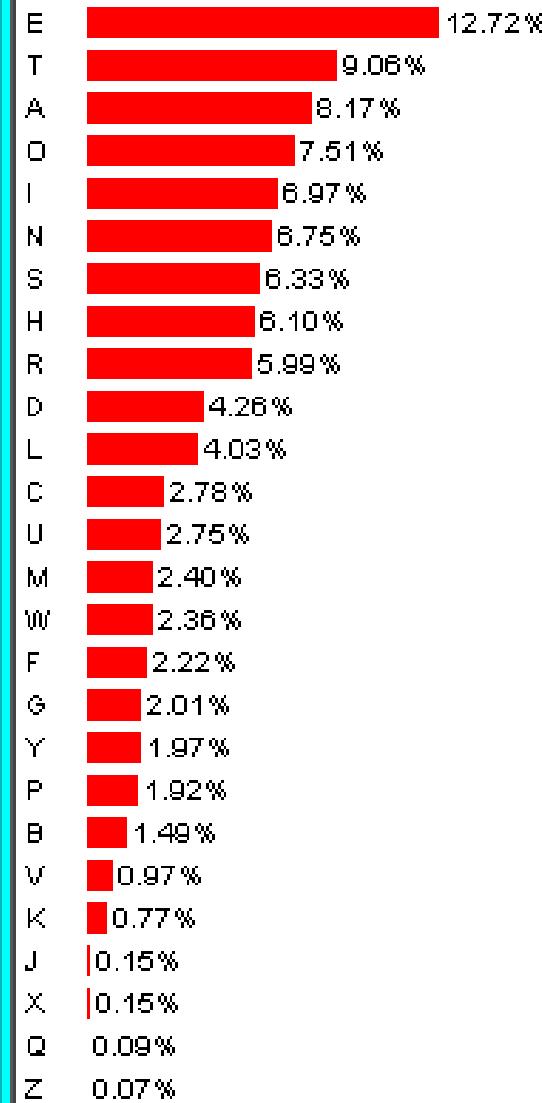


Break Substitution Cipher: Frequency Analysis

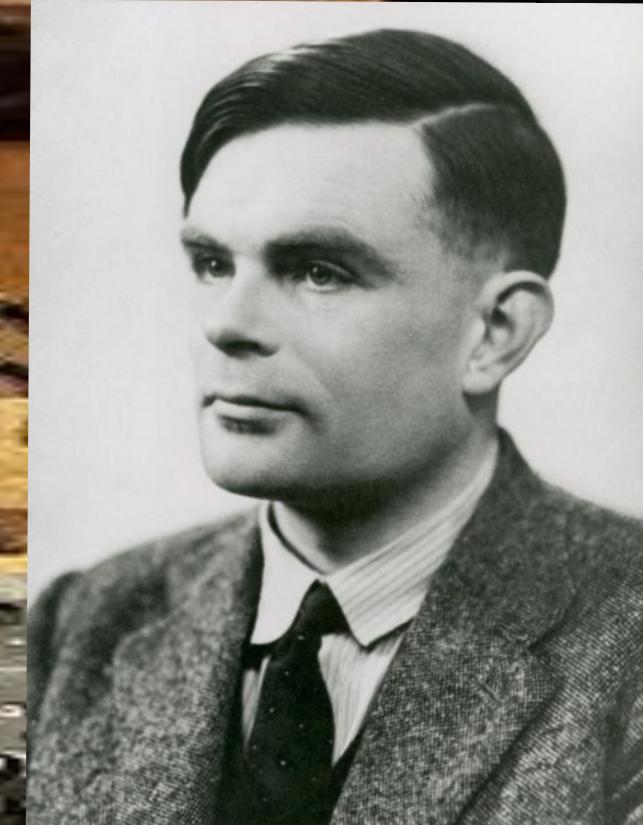
Input text letter frequencies:



English text letter frequencies:



The Enigma



Broken by British
in an effort led by Turing

Agenda

1. Crypto Usage & Goals

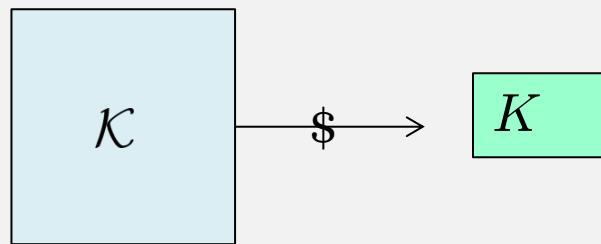
2. Classical Crypto

3. One-time Pad & Perfect Secrecy

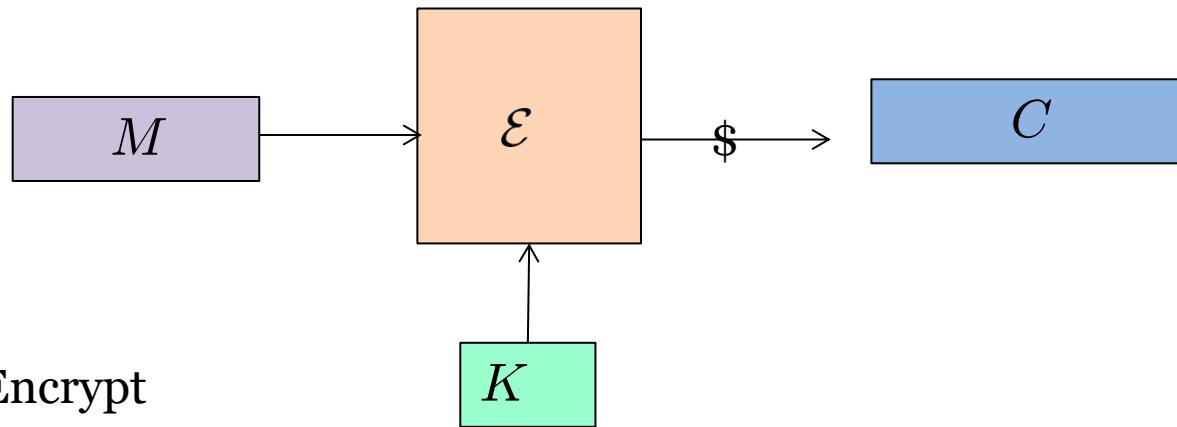
4. Modern Crypto

Encryption Syntax

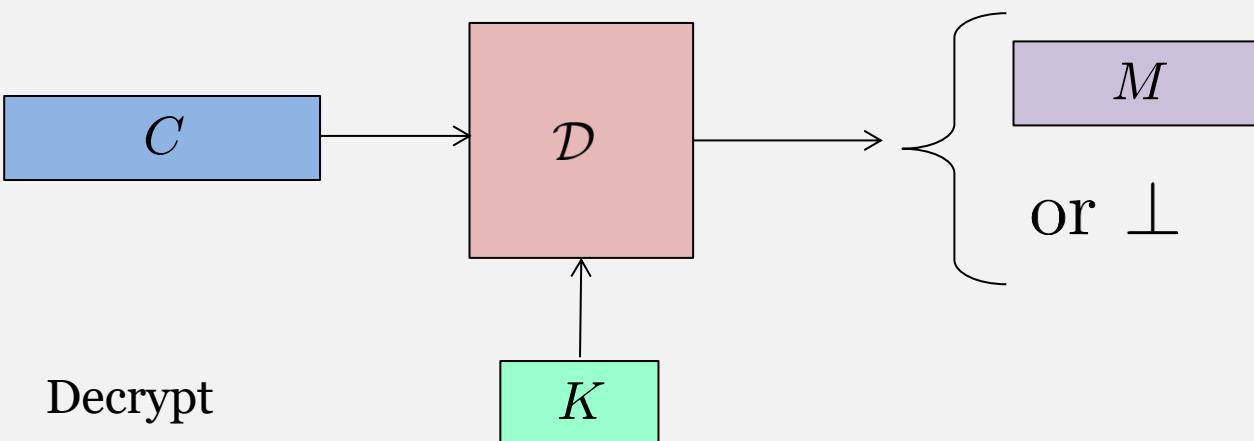
Key Gen



Encrypt



Decrypt



Define security?



Perfect Secrecy

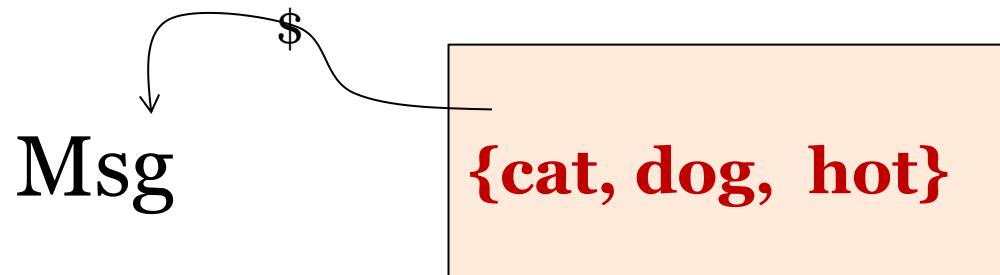
Intuition: Ciphertext should reveal **no additional info** about plaintext

For every m and c :

$$\Pr_{K \leftarrow \mathcal{K}}[\text{Msg} = m \mid \mathcal{E}_K(\text{Msg}) = c] = \Pr[\text{Msg} = m]$$

Common case: Ciphertext is uniformly random, independent of msg

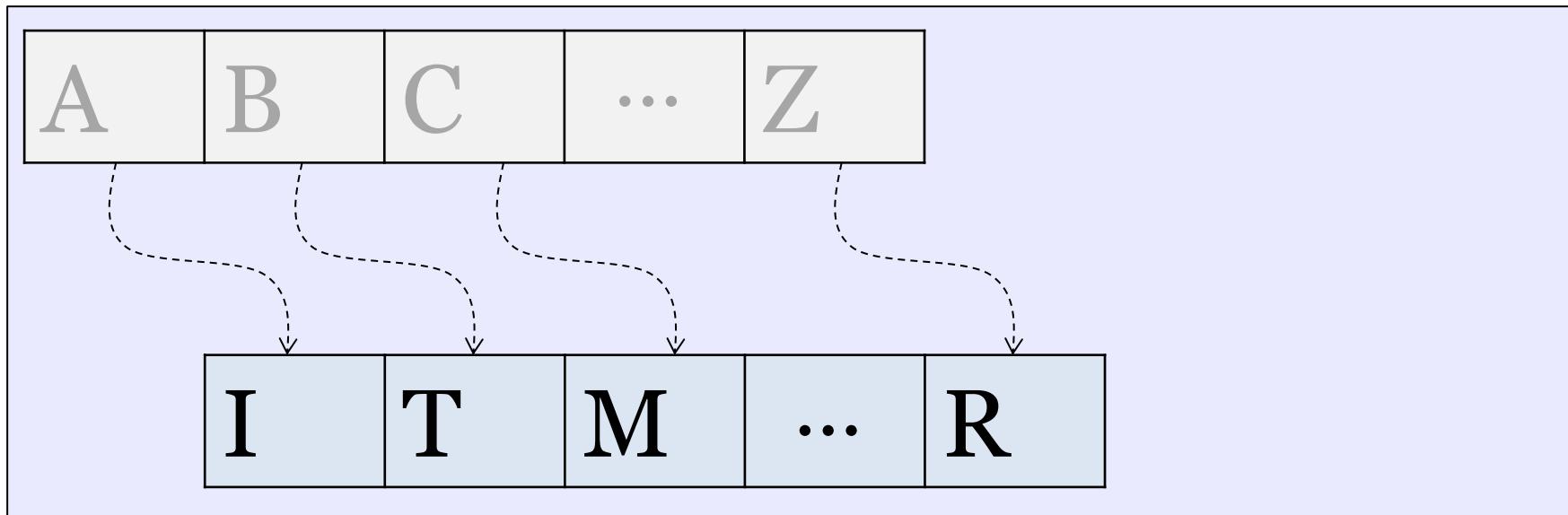
An Example



A large gray downward-pointing arrow is positioned between the context cracking diagram and the mathematical analysis below. To the right of the arrow, the text "Not perfectly secure" is written.

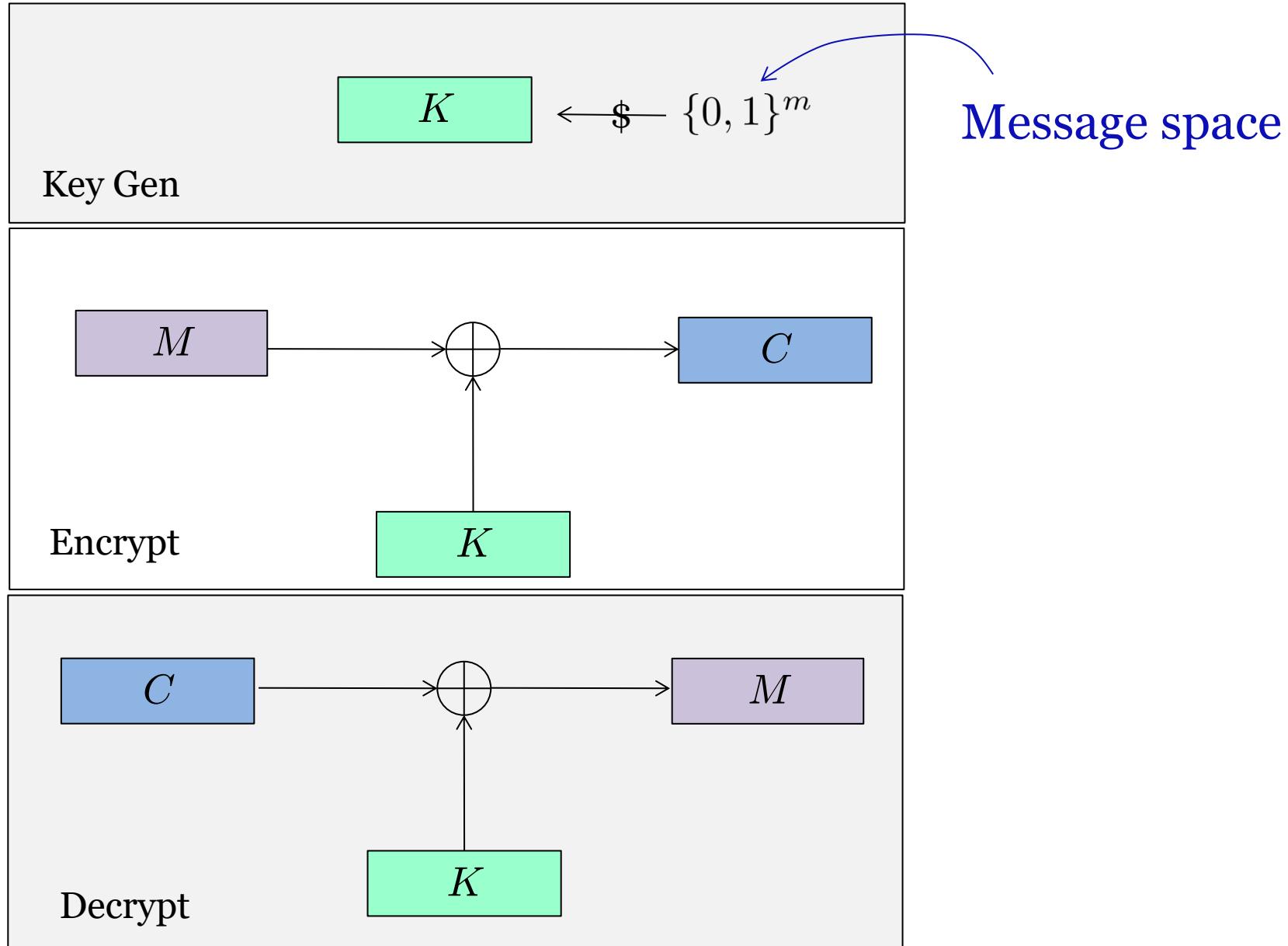
$$\Pr[\text{Msg} = \text{dog} \mid \text{Ctx}] = \frac{1}{2} \neq \Pr[\text{Msg} = \text{dog}] = \frac{1}{3}$$

Substitution Cipher Is Not Perfectly Secret



$$\Pr[\text{Msg} = \text{bad boy} \mid \text{Ctx}] = 1 \neq \Pr[\text{Msg} = \text{bad boy}] = 1/2$$

Achieving Perfect Secrecy: One-time Pad



Behind Every Notion, There Is An Assumption

For every m and c :

$$\Pr_{K \leftarrow \mathcal{K}}[\text{Msg} = m \mid \mathcal{E}_K(\text{Msg}) = c] = \Pr[\text{Msg} = m]$$

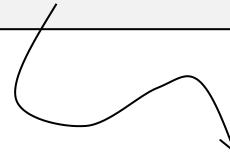


It's **assumed** that you pick a fresh key for each encryption

Reusing One-time Pad Breaks Security



One can obtain $M \oplus M'$ via $C \oplus C'$



Can recover both M and M' if the messages
are English texts and long enough

THE VENONA SECRETS

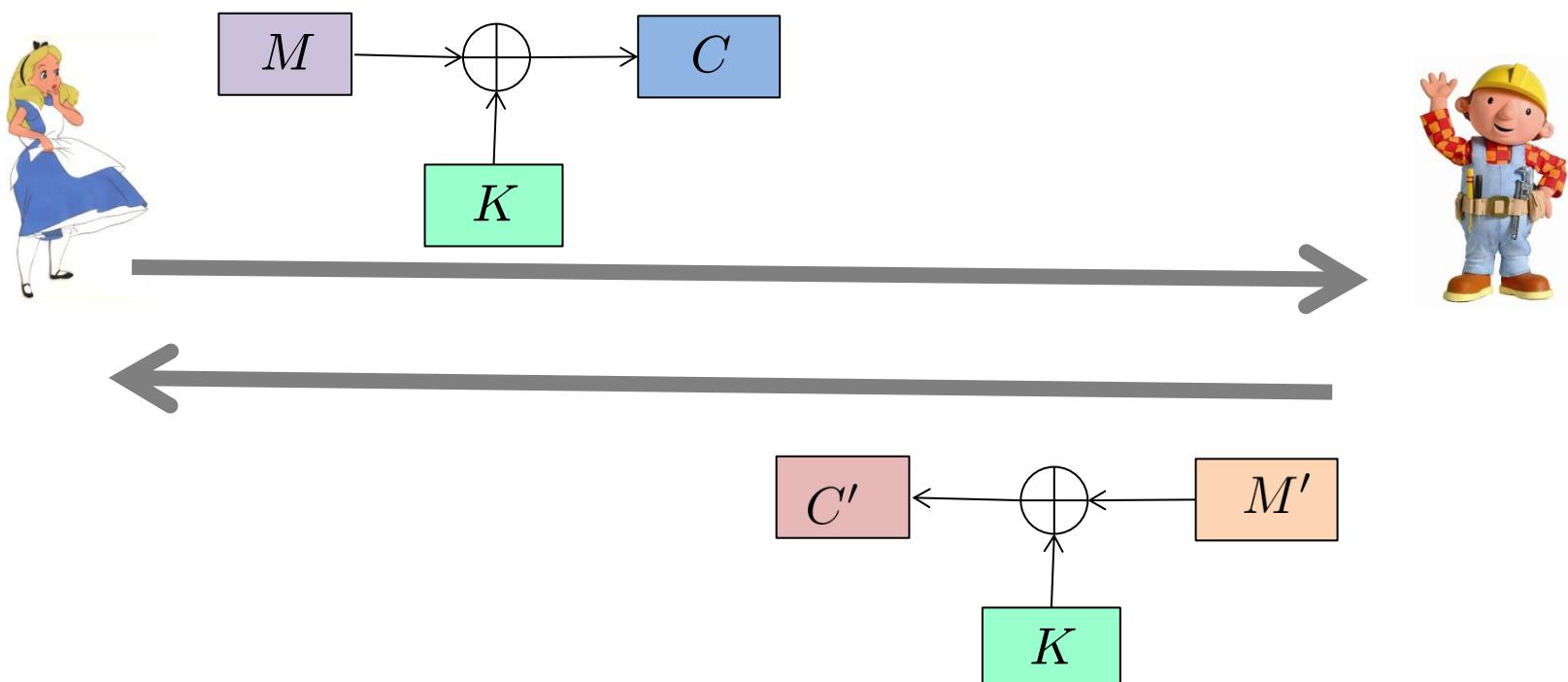
The Definitive Exposé of
Soviet Espionage in America

Bad Usage of One-time Pad: USSR's reusing of one-time pads led to the decryption of 2900 messages.



Bad Usage of One-time Pads:

PPTP protocol in Windows NT



Nov 26, 2019

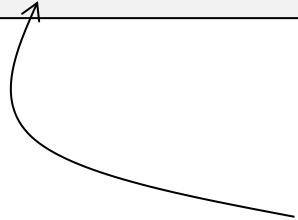
FORTINET PRODUCTS USED HARDCODED ENCRYPTION KEY

By Dennis Fisher

Fortinet's blunder led them to reuse a one-time pad several times

Limitation of Perfect Secrecy

If $|\mathcal{M}| > |\mathcal{K}|$ then **no** scheme is perfectly secret



Impractical

Agenda

1. Crypto Usage & Goals

2. Classical Crypto

3. One-time Pad & Perfect Secrecy

4. Modern Crypto

Lego Approach

**Computational
Science**

**Modern
Crypto**

Provable Security

Modern Crypto: A Lego Approach

Primitives:

AES

SHA-2

Factoring

...

Transformers

Applications:

Encryption

MAC

Digital Signature

Modern Crypto: A Computational Science

- Assume **computational** hardness of **a few** primitives

AES

SHA-2

Factoring

...

- Confidence by cryptanalysis

Modern Crypto: Provable Security

- Define** security notions for applications
- Prove** the transformer meets the notions

