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

Bank of America

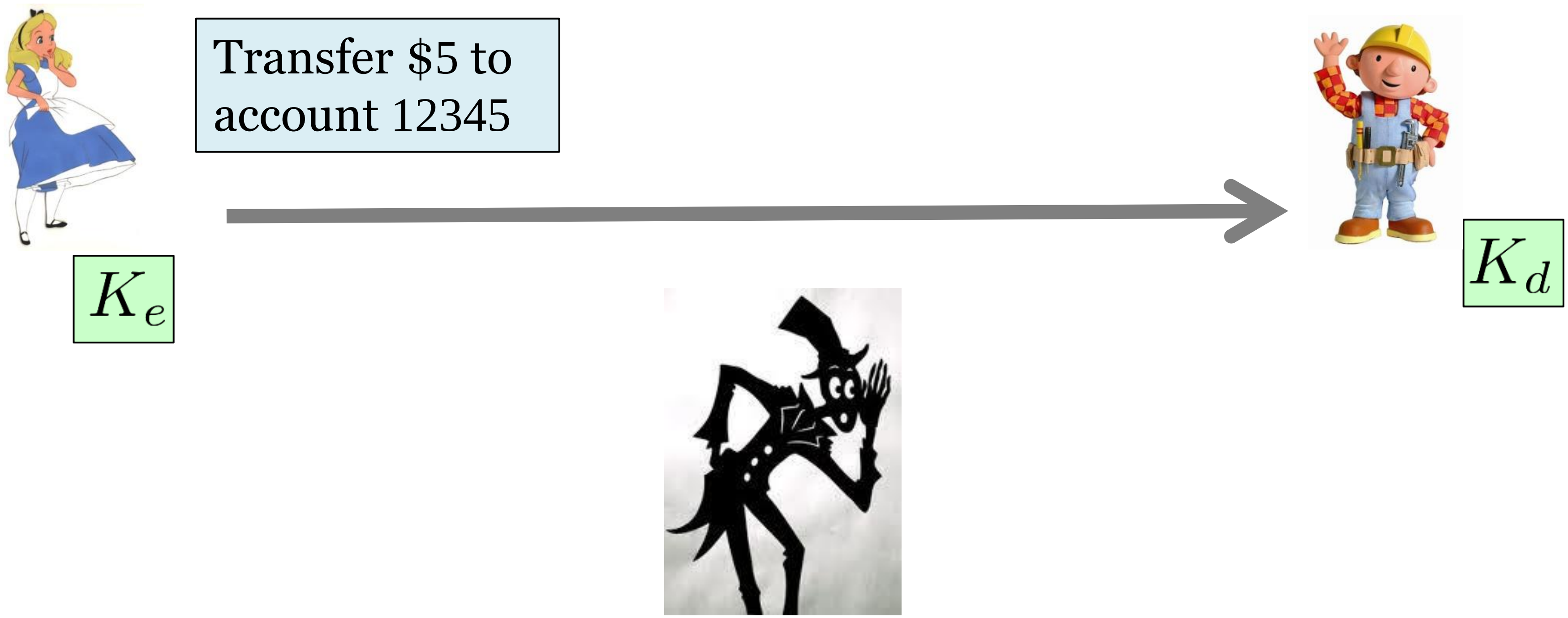
Secure messaging

WhatsApp

Bitcoin

Tor

A Classical Crypto Goal: Privacy



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

A Classical Crypto Goal: Privacy

1100000100101
0101011110111

K_d

K_e

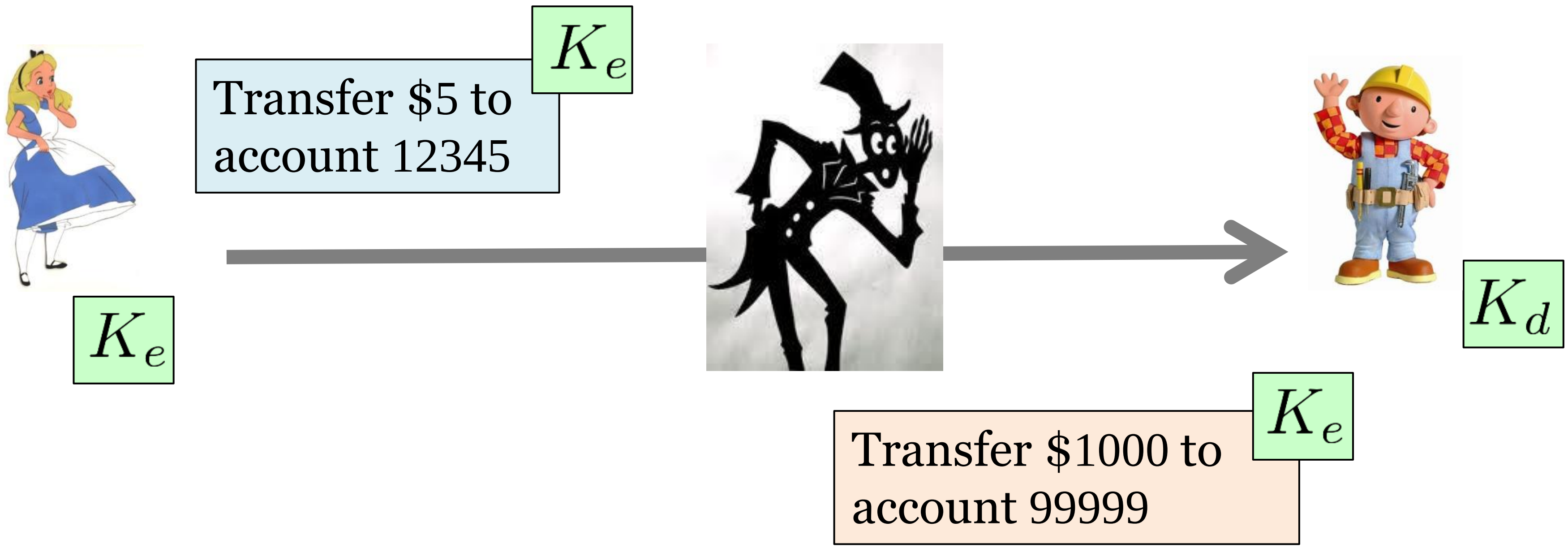
Private-key setting: $K_e = K_d$

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

	Privacy	Authenticity
Private key	**Private-key Enc**	**MAC**
Public key	**Public-key Enc**	**Digital Signature**

Agenda

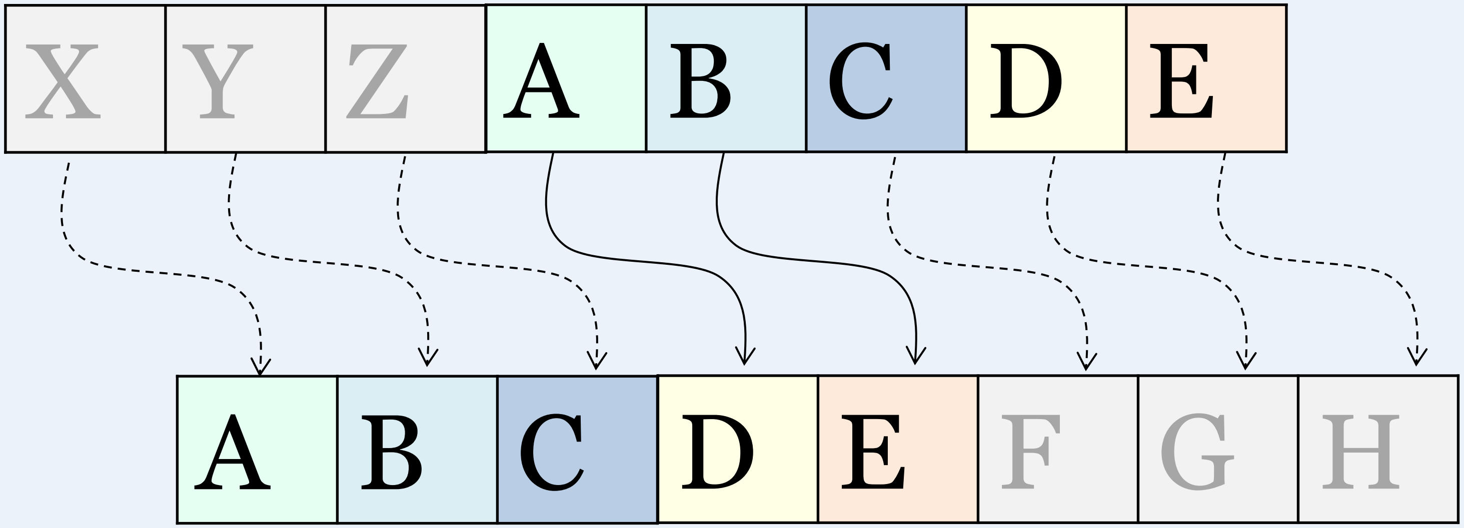
1. Crypto Usage & Goals

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

The Register®

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.

The Register®

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 $K \in \{0, \ldots, 25\}$

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

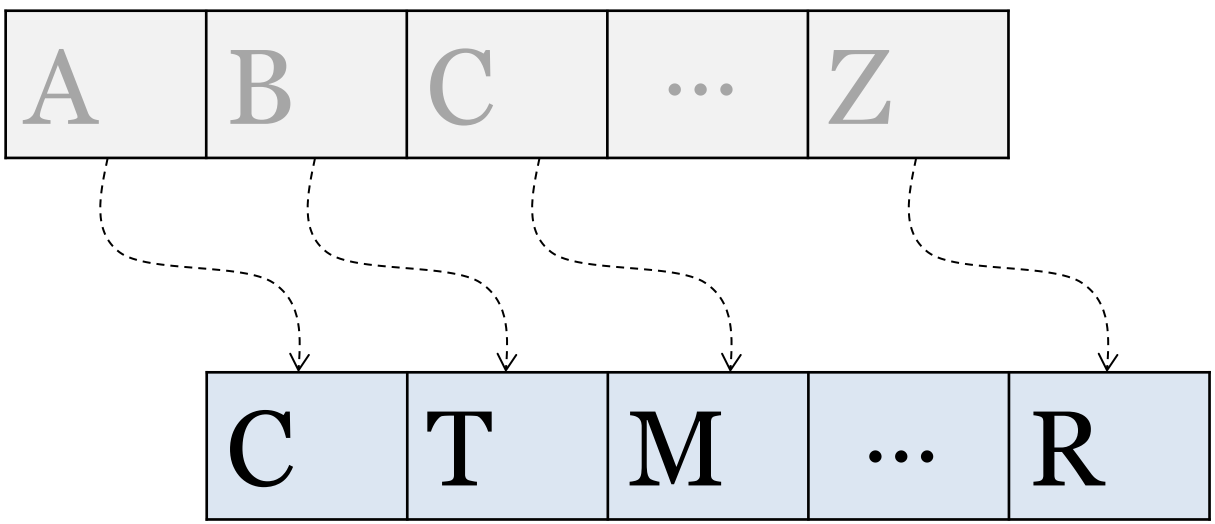
Small Keyspace

Broken by brute force

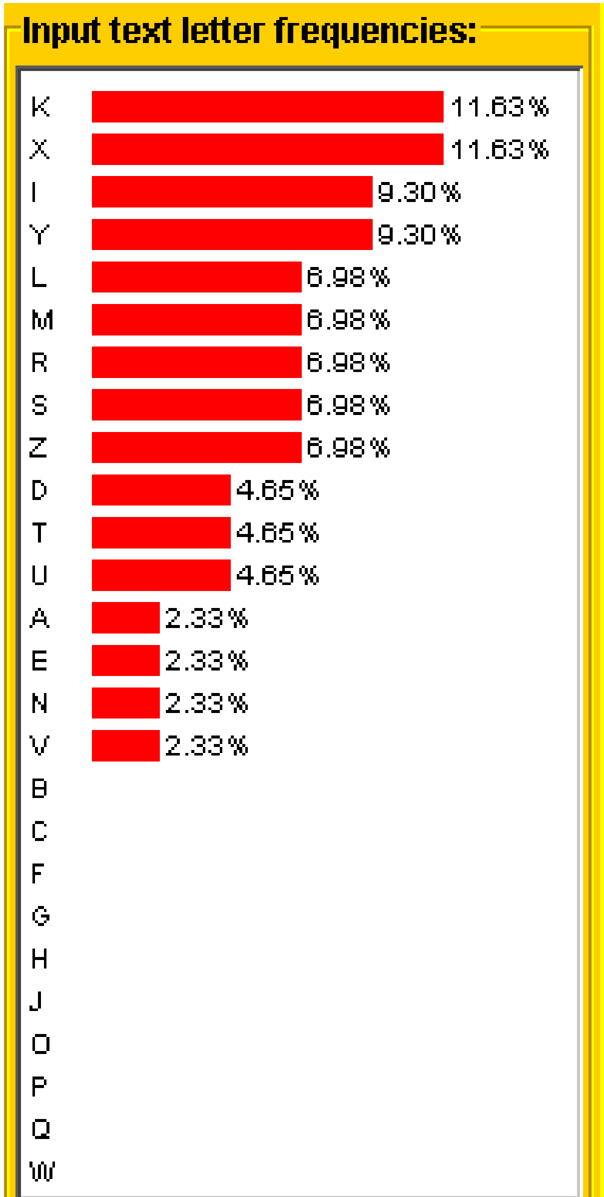
Substitution Cipher

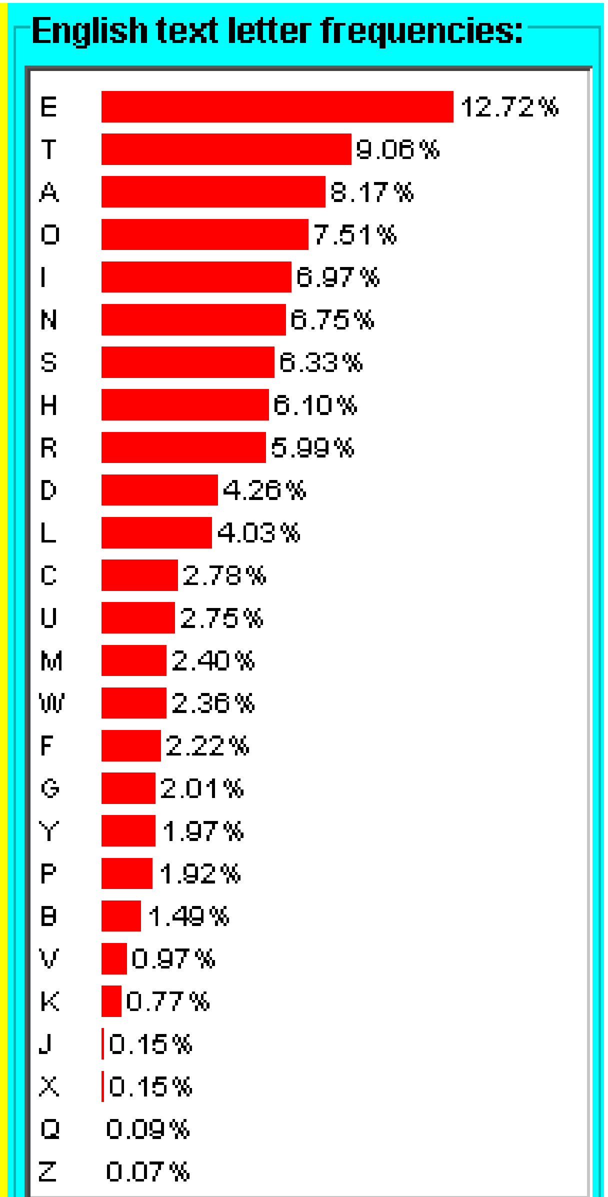
Key: a permutation $\pi : \Sigma \to \Sigma$

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

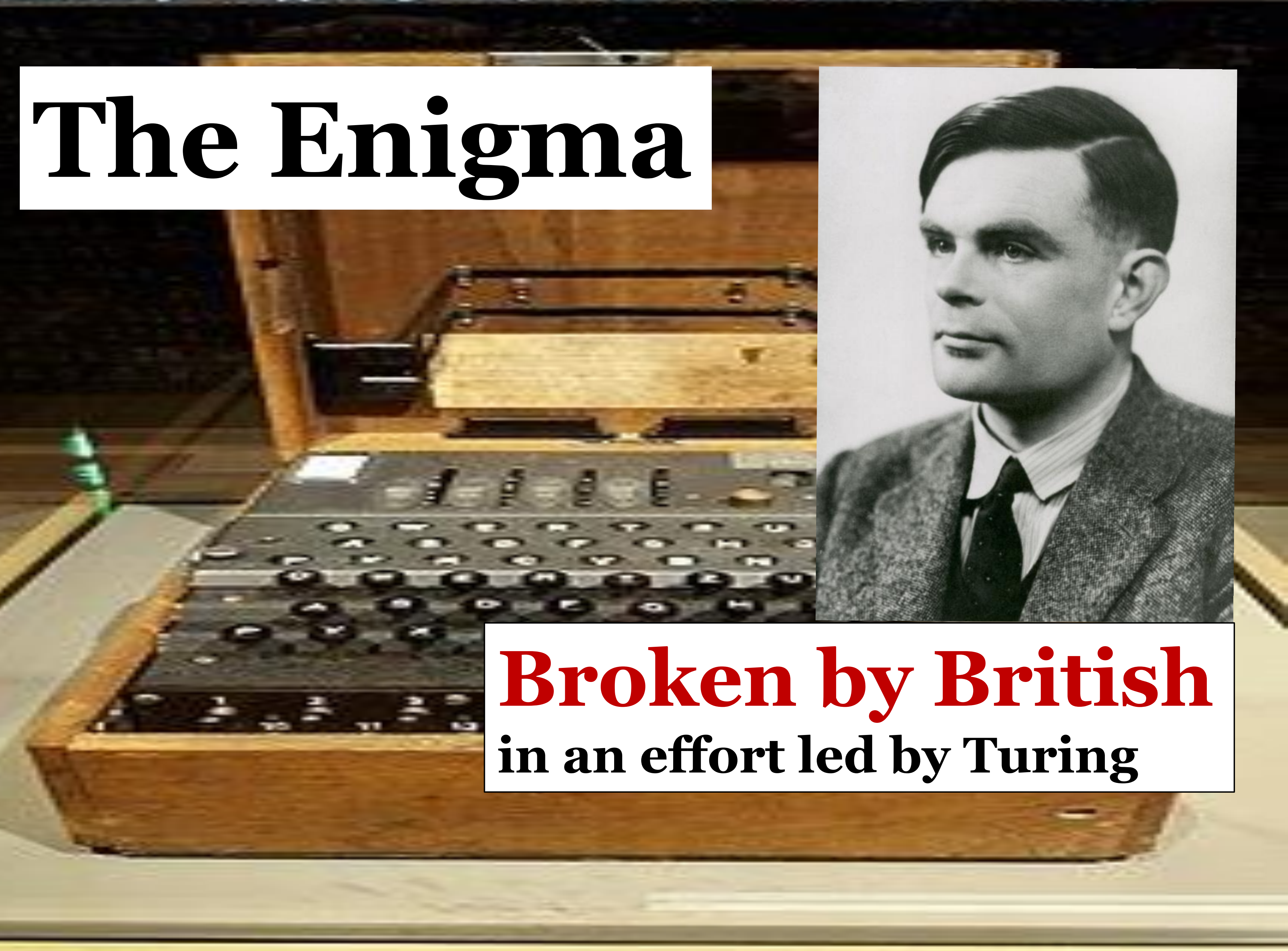


Break Substitution Cipher: Frequency Analysis





The Enigma



Broken by British

in an effort led by Turing

Agenda

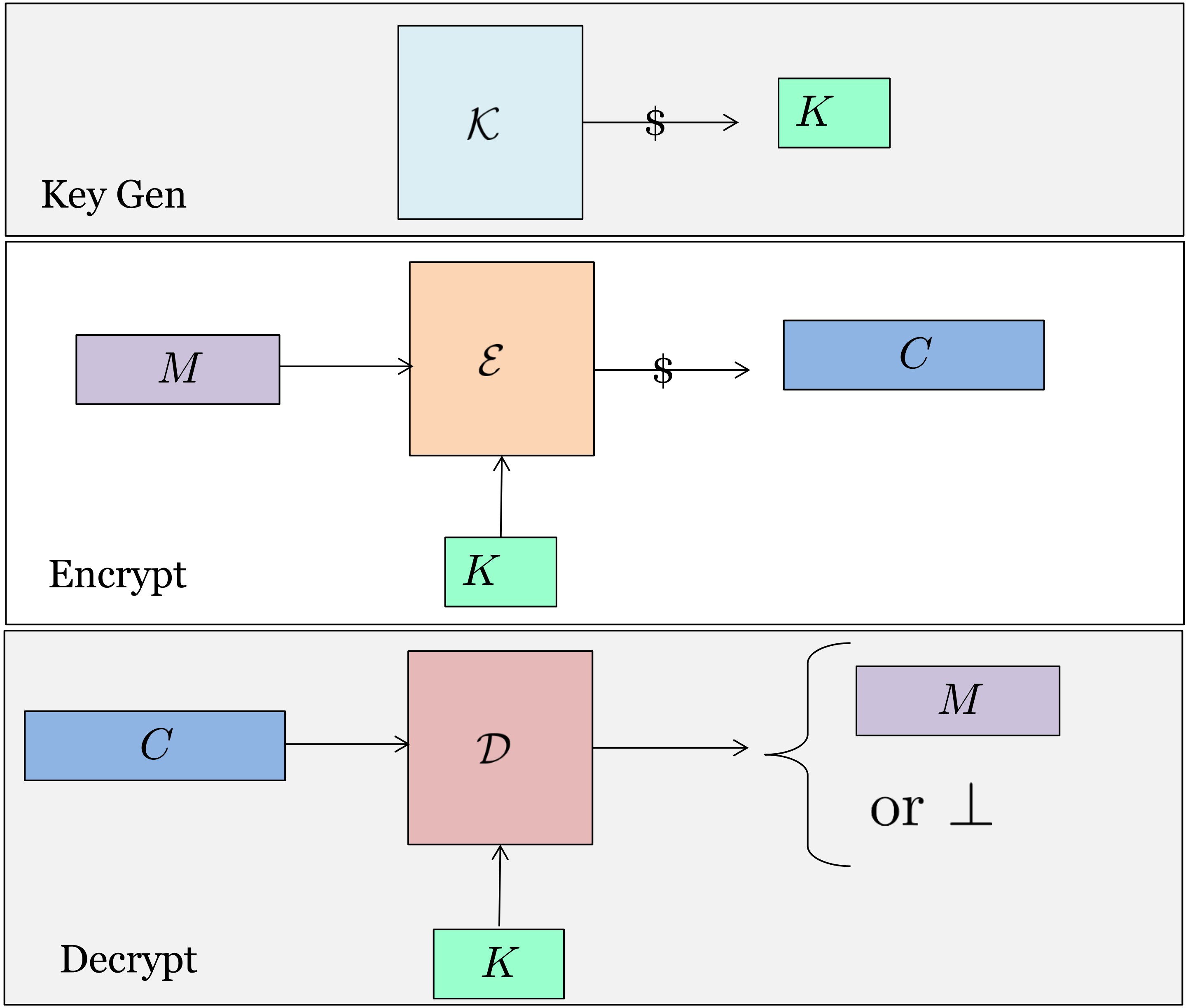
1. Crypto Usage & Goals

2. Classical Crypto

3. **One-time Pad & Perfect Secrecy**

4. Modern Crypto

Encryption Syntax



Define security?

Perfect Secrecy

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

For every m and c:

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

Common case: Ciphertext is uniformly random, independent of msg

An Example

$

Msg

{cat, dog, hot}

Ctx

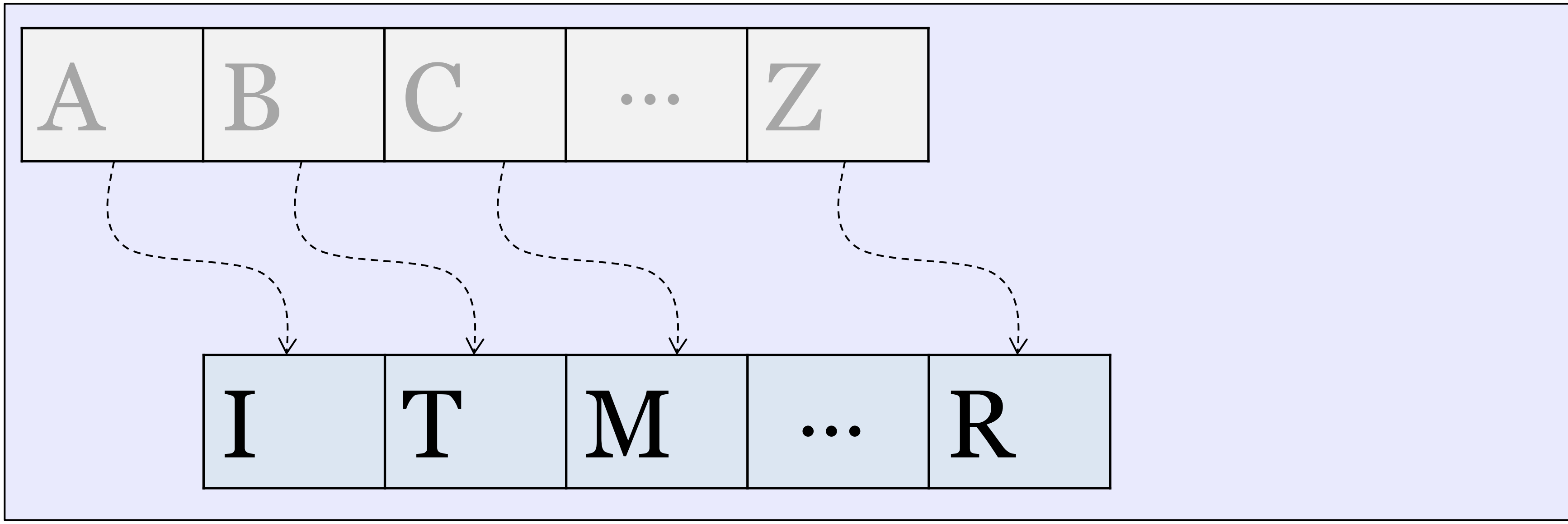
cracked

Msg = *o*

Not perfectly secure

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

Substitution Cipher Is Not Perfectly Secret

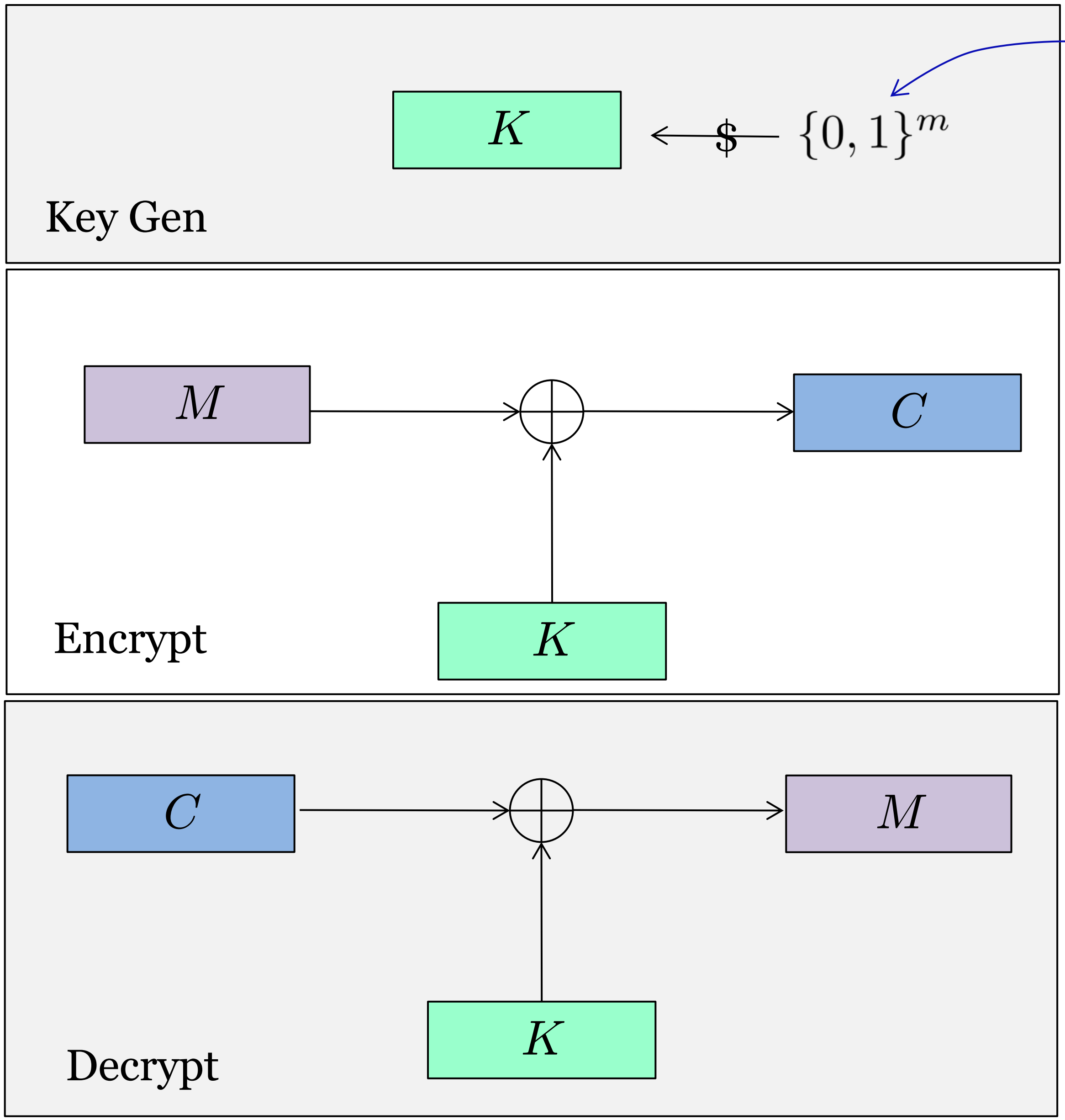


Msg $\xleftarrow{\$}$ **{hot day, bad boy}**

Ctx = "tic tok"

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

Achieving Perfect Secrecy: One-time Pad



Message space

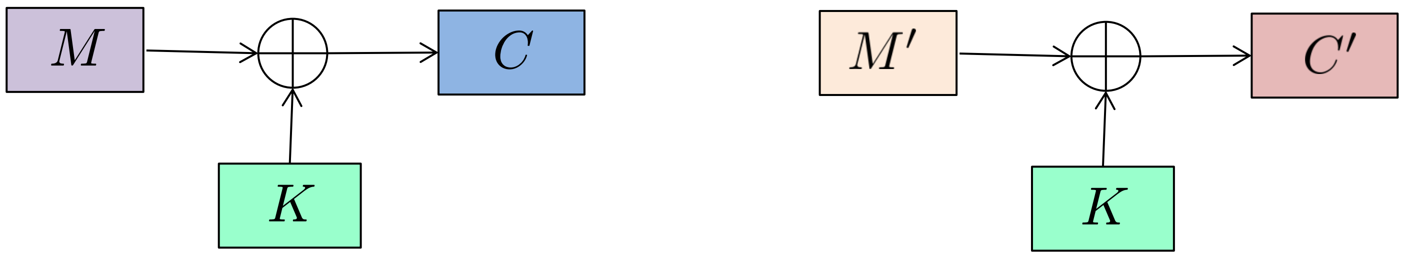
Behind Every Notion, There Is An Assumption

For every m and c:

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

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

Reusing One-time Pad Breaks Security



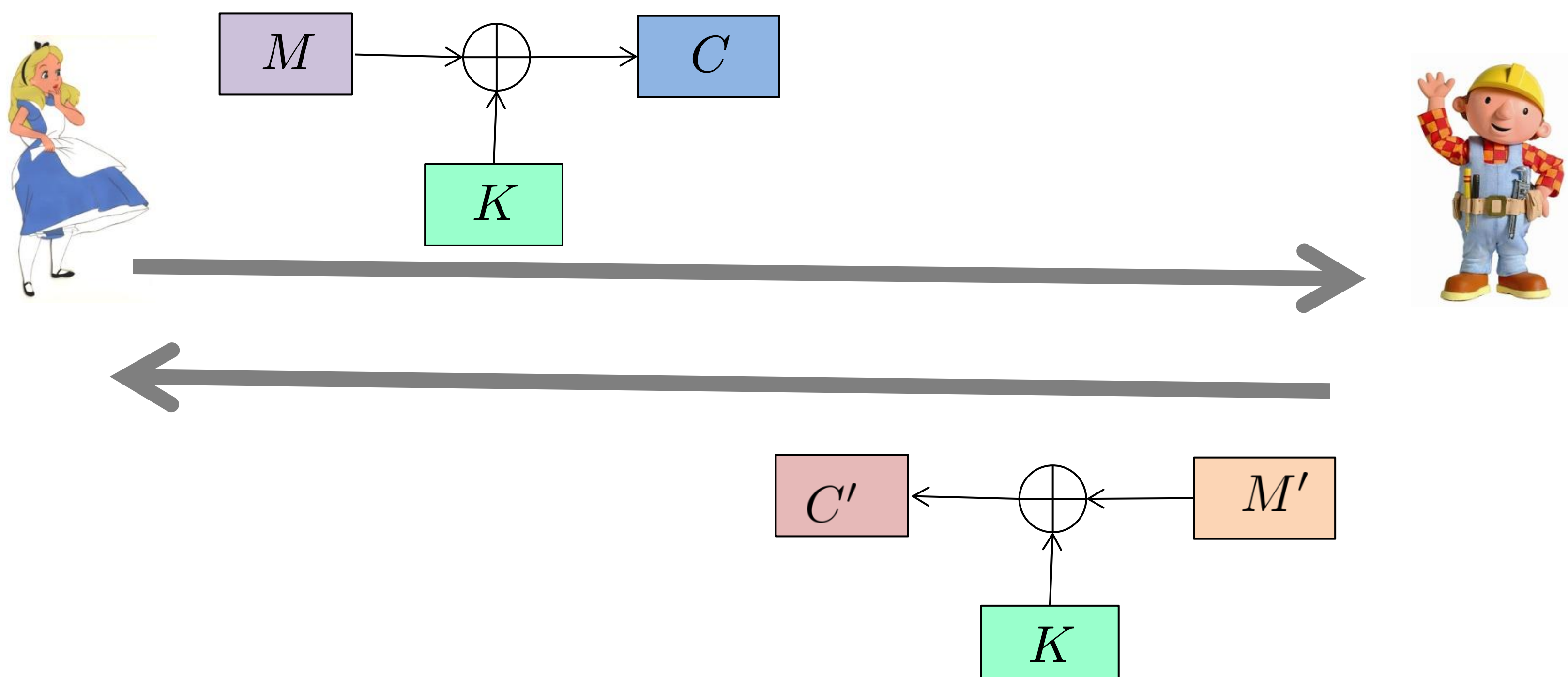
One can obtain $M \oplus M'$ via $C \oplus C'$

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

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



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