Symmetric Encryption: Defining Security and Perfectly Secure Cipher

Yan Huang

Credits: Vitaly Shmatikov (Cornell Tech)
Dan Boneh (Stanford)

Announcement (CACR Talk)

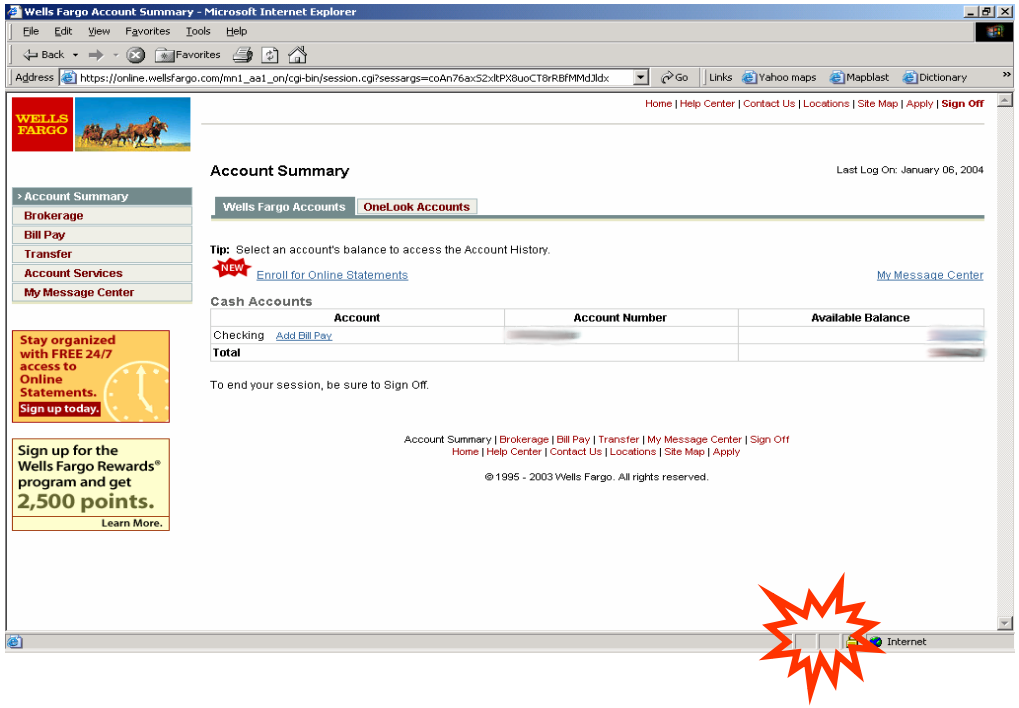
Towards More Secure and Usable Passwords

Thursday 12:00-1:00 (Law 335)

Dr. Lujo Bauer, Carnegie Mellon University

(Pizza and drink provided)

Secure communication



HTTPS

no eavesdropping

no tampering

Secure Sockets Layer / TLS

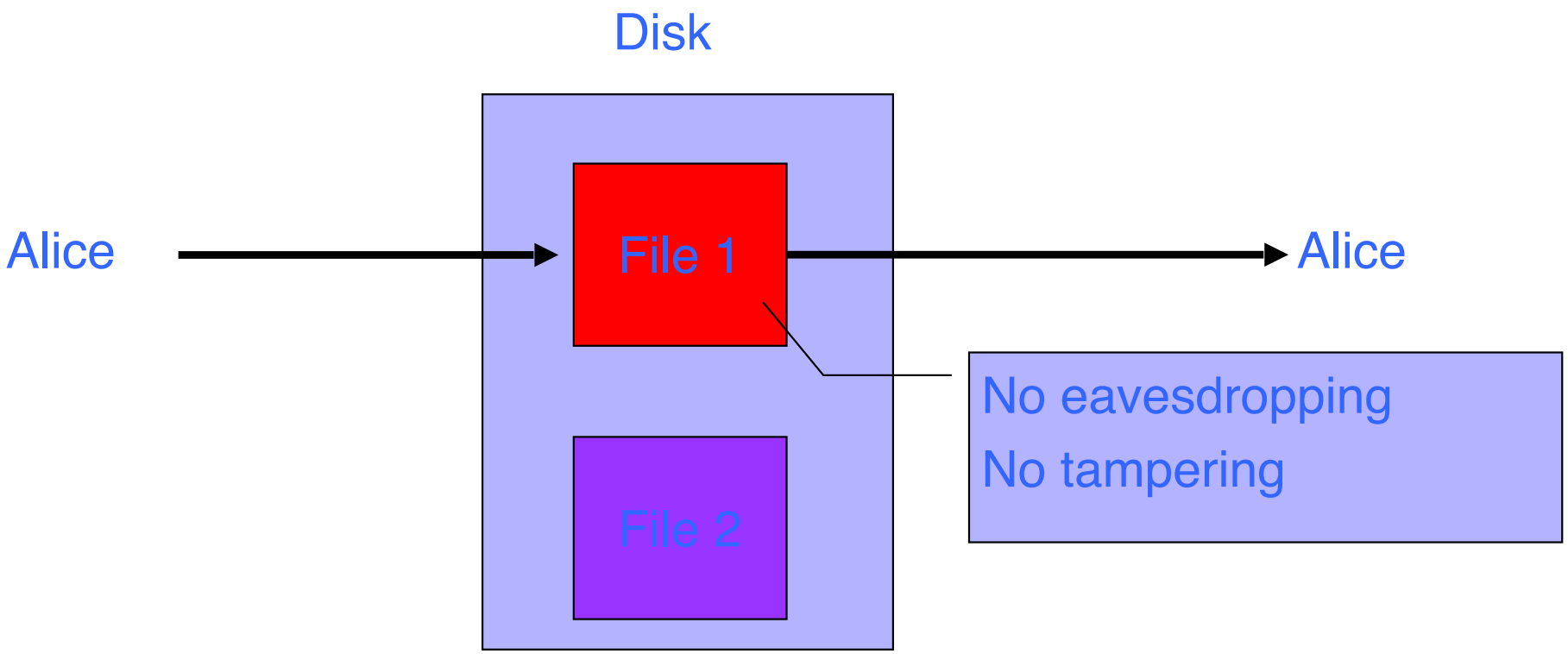
Two main parts

1. Handshake Protocol: Establish shared secret key using public-key cryptography

2. Transmit data using shared secret key

   Ensure confidentiality and integrity

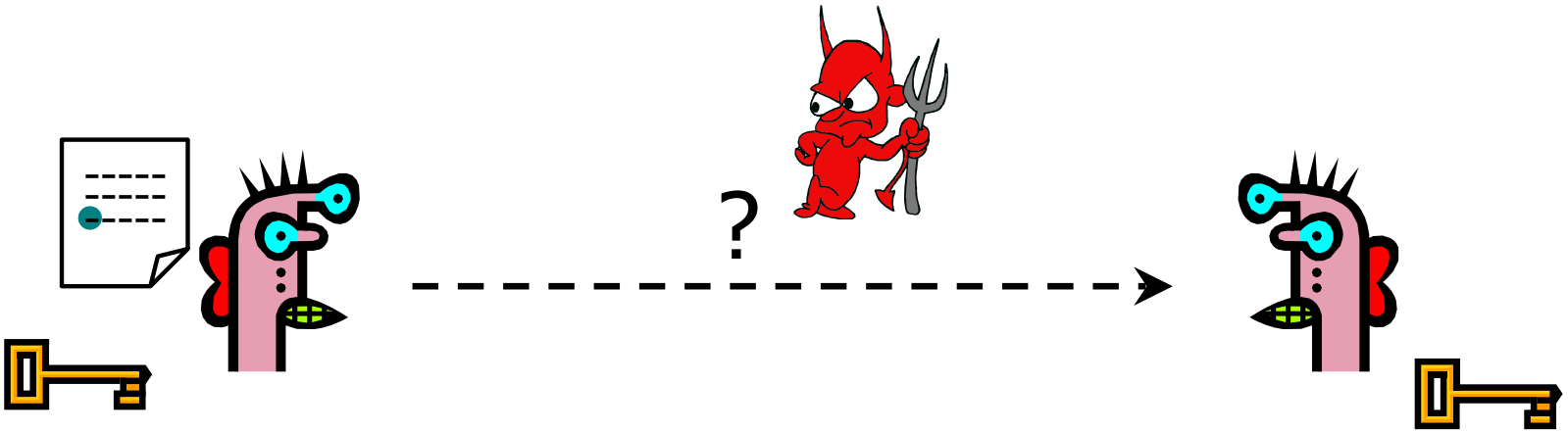
Protected files on disk



Analogous to secure communication:

Alice today sends a message to Alice tomorrow

Basic Problem



Given: both parties already know the same secret

Goal: send a message confidentially

How is this achieved in practice?

Kerckhoffs's Principle

- An encryption scheme should be secure even if enemy knows everything about it except the key
  - Attacker knows all algorithms
  - Attacker does not know random numbers
- Do not rely on secrecy of the algorithms ("security by obscurity")

Easy lesson:
use a good random number generator!

Randomness Matters!

The New York Times

Business Day
Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | A

Flaw Found in an Online Encryption Method

By JOHN MARKOFF
Published: February 14, 2012

SAN FRANCISCO — A team of European and American mathematicians and cryptographers have discovered an unexpected weakness in the encryption system widely used worldwide for online shopping, banking, e-mail and other Internet services intended to remain private and secure.

RECOMMEND
TWITTER
LINKEDIN
COMMENTS (127)
E-MAIL
PRINT
SINGLE PAGE
REPRINTS

Readers' Comments

Readers shared their thoughts on this article.

Read All Comments (127) »

The flaw — which involves a small but measurable number of cases — has to do with the way the system generates random numbers, which are used to

Internet users, there is nothing a
sites will need to make changes t
said

› Uptime | IT and business computing insights

Crypto shocker: four of every 1,000 public keys provide no security (updated)

By Dan Goodin | Published 7 days ago

What is a secure cipher?

Attacker's abilities: obtains one ciphertext (for now)

Possible security requirements:

attempt #1: attacker cannot recover secret key

$$E(k,m)=m$$

attempt #2: attacker cannot recover the plaintext

$$E(k,m_0||m_1)=m_0||m_1 \oplus k$$

Shannon's idea:

Ciphertext should reveal no "info" about Plaintext

Shannon's perfect secrecy

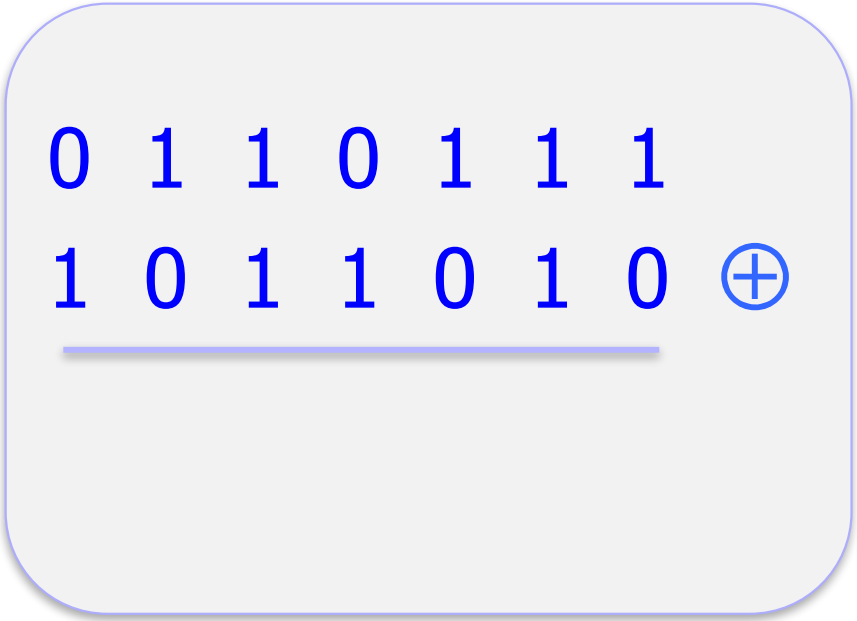
Let (E, D) be a cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$

(E,D) has perfect secrecy if $\forall\, m_0, m_1 \in \mathcal{M}$, $|m_0| = |m_1|$

$\{ E(k,m_0) \} = \{ E(k,m_1) \}$ where $k \leftarrow \mathcal{K}$.

Review: XOR

XOR of two strings in $\{0,1\}^n$ is their bit-wise addition mod 2



An Important Property of XOR

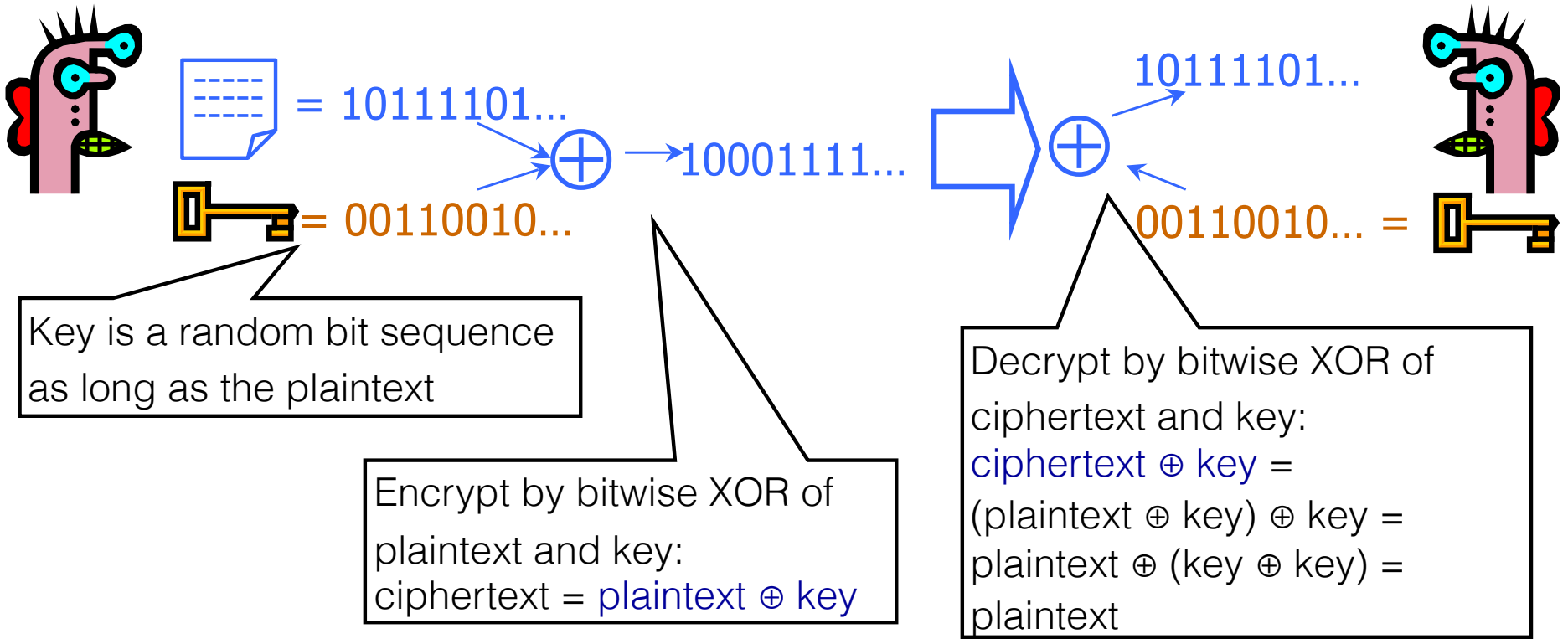
Thm: Let Y be a random variable over $\{0,1\}^n$, X an independent uniform random variable on $\{0,1\}^n$

Then $Z := Y \oplus X$ is uniform variable on $\{0,1\}^n$

Proof: (for n=1)

$$\begin{aligned}
\Pr[\, Z=0 \,] &= \Pr[\, Y=0 \wedge X=0 \textbf{ or } Y=1 \wedge X=1] \\
&= \Pr[\, Y=0 \wedge X=0] + \Pr[Y=1 \wedge X=1] \\
&= \Pr[\, Y=0] \cdot \Pr[X=0] + \Pr[Y=1] \cdot \Pr[X=1] \\
&= \Pr[\, Y=0] \cdot (1/2) + \Pr[Y=1] \cdot (1/2) \\
&= (\Pr[\, Y=0] + \Pr[Y=1]) \cdot (1/2) = \Pr[\, Z=1 \,]
\end{aligned}$$

One-Time Pad (Vernam Cipher)



Cipher achieves perfect secrecy if and only if there are as many possible keys as possible plaintexts, and every key is equally likely (Claude Shannon, 1949)

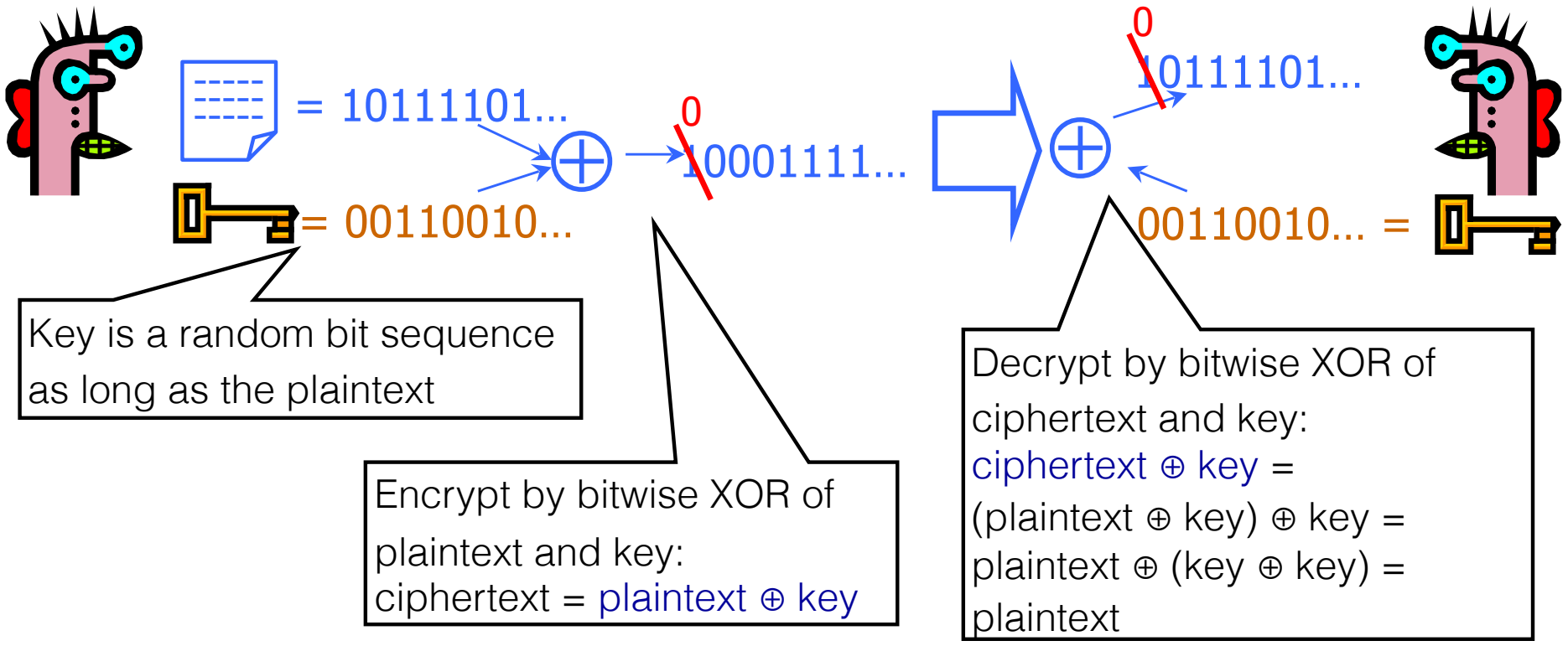
Advantages of One-Time Pad

- Easy to compute
  - Encryption and decryption are the same operation
  - Bitwise XOR is very cheap to compute
- As secure as theoretically possible
  - Given a ciphertext, all plaintexts are equally likely, regardless of attacker's computational resources
  - …if and only if the key sequence is truly random
    - True randomness is expensive to obtain in large quantities
  - …if and only if each key is as long as the plaintext
    - But how do the sender and the receiver communicate the key to each other? Where do they store the key?

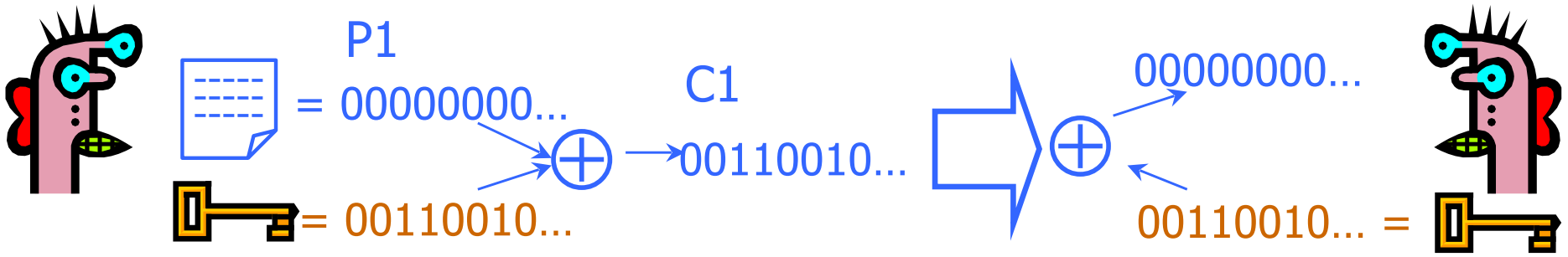
Problems with One-Time Pad

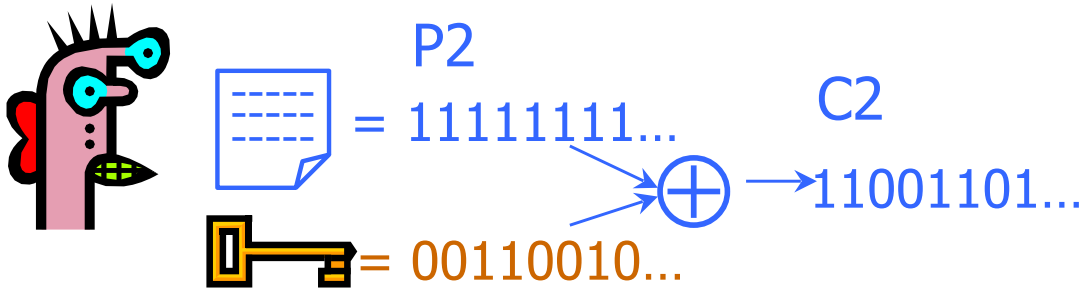
- Key must be as long as the plaintext
  - Impractical in most realistic scenarios
  - Still used for diplomatic and intelligence traffic
- Does not guarantee integrity
  - One-time pad only guarantees confidentiality
  - Attacker cannot recover plaintext, but can easily change it to something else
- Insecure if keys are reused
  - Attacker can obtain XOR of plaintexts

No Integrity



Dangers of Reuse

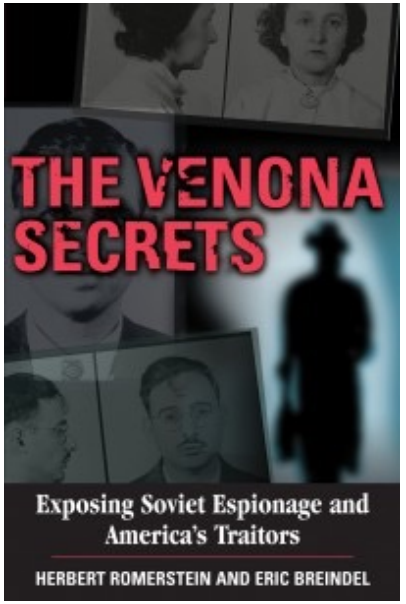




Learn relationship between plaintexts

C1⊕C2 = (P1⊕K)⊕(P2⊕K) =

(P1⊕P2)⊕(K⊕K) = P1⊕P2



Reading Assignment

- Read Kaufman 2.1-4 and 4.2