Gems of TCS

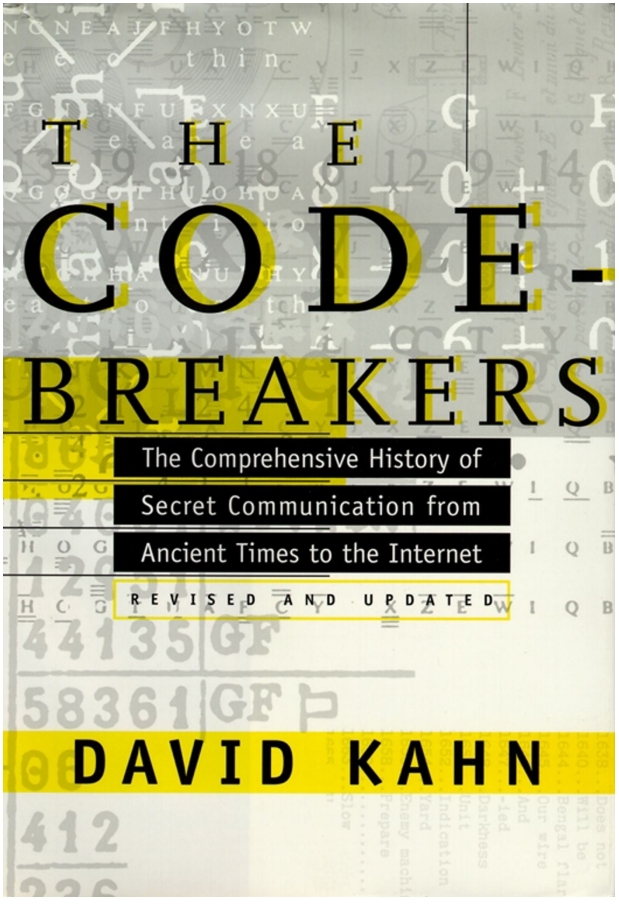
Introduction to Cryptography

Symmetric Encryption
Secret key Encryption

Sasha Golovnev

April 13, 2021

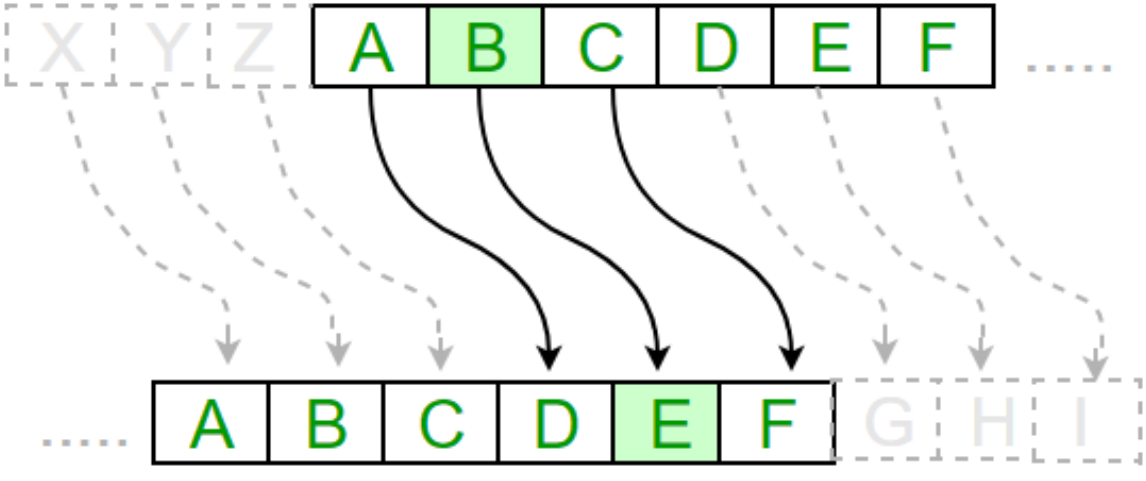
The Codebreakers



Pig Latin

emsgay ofyay eorythay

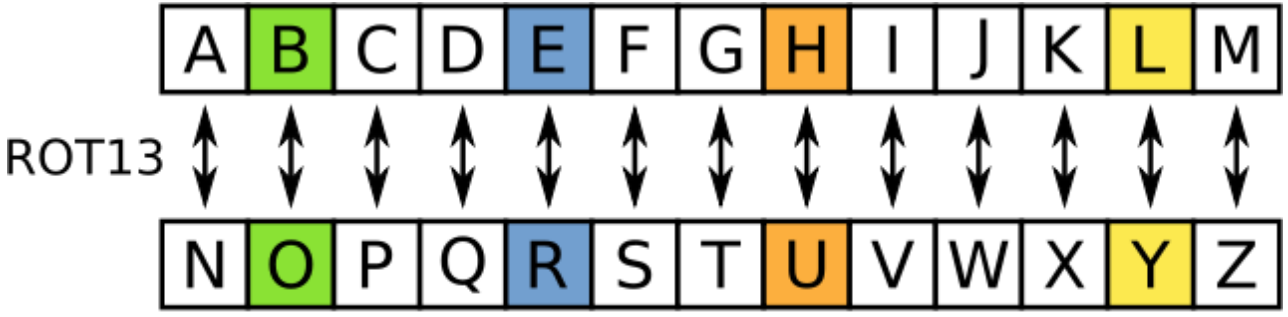
Caesar Cipher

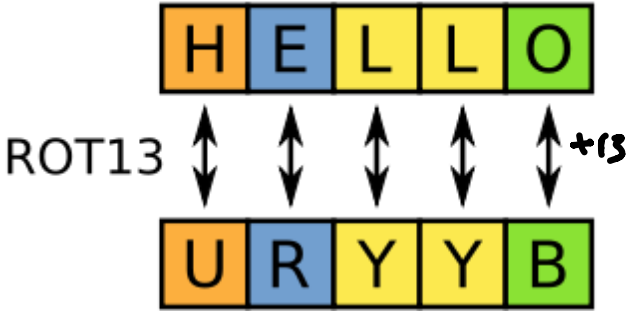


CAT $\xrightarrow{+3}$ FDW

CAT $\xleftarrow{-3}$

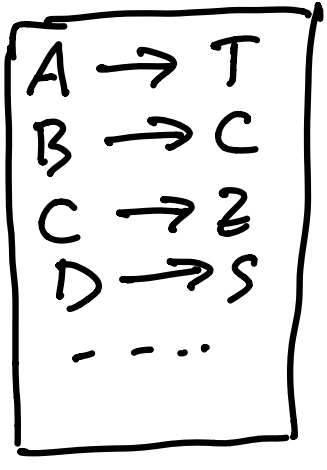
ROT13



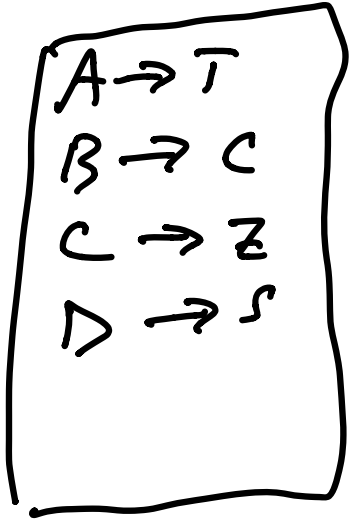


Substitution Ciphers

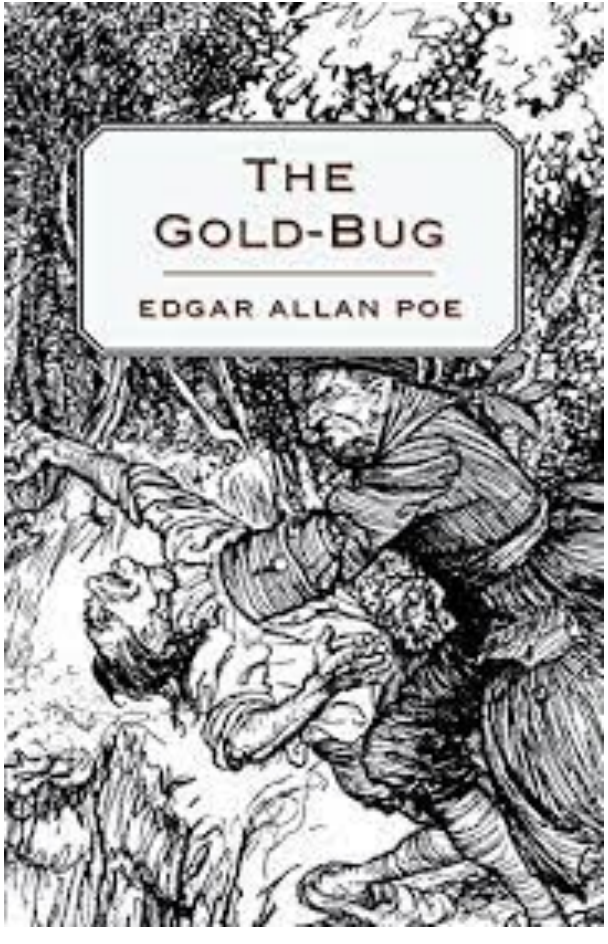
Alice



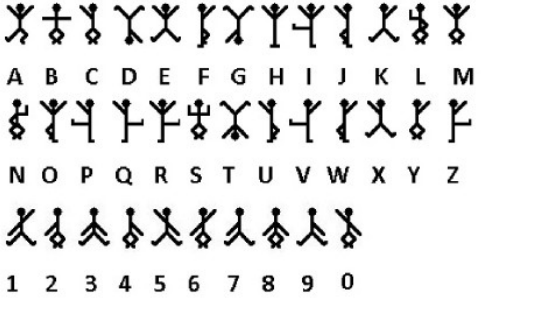
Bob



Breaking Substitution Ciphers



Dancing Man Code
(Sherlock Holmes)



English language is redundant

Letter Frequency

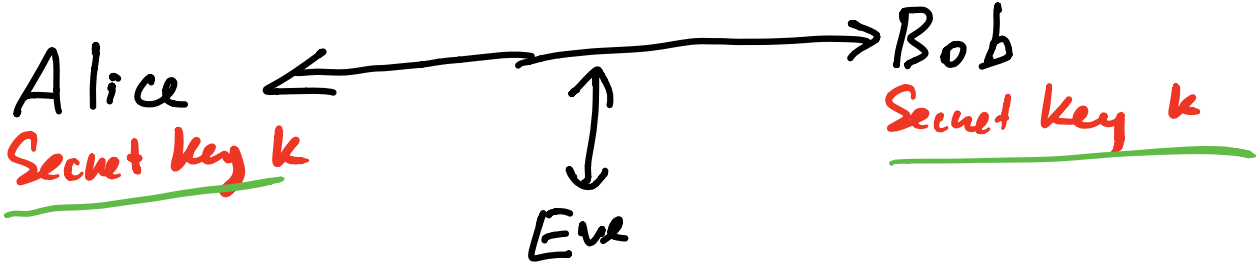
Frequencies of pairs letters
he th ---

e	13%
t	9.1%
a	8.2%
o	7.5%
i	7%
n	6.7%
s	6.3%
h	6.1%
r	6%
d	4.3%
l	4%
c	2.8%
u	2.8%
m	2.4%
w	2.4%
f	2.2%
g	2%
y	2%
p	1.9%
b	1.5%
v	0.98%

Demonstration

qvv jds jqosu yqcw al jds qisnqes qtsnczqg qns
uysgj al jds ebisngtsgj cg vsuu jdqg q uszbgw

Good Cipher



If they don't have secret, then $m \rightarrow c$

"ATTACK" → "010011"

Next time Eve sees "010011"

"ATTACK"

Cipher is pair algs (E, D)

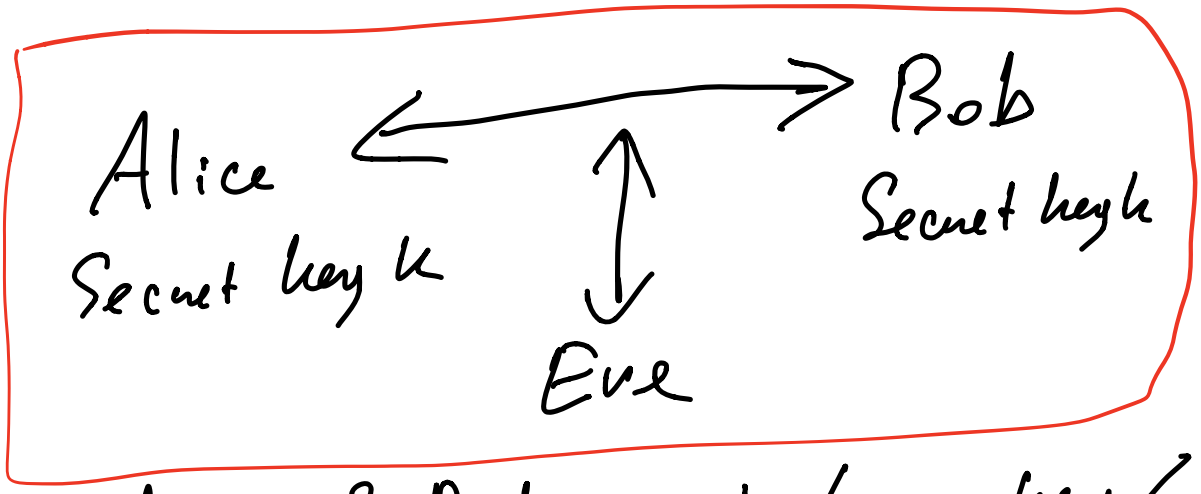
$E(k, m) \rightarrow c$

$D(k, c) \rightarrow m$

1. Correctness:

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

Secret key Cryptography



1. Alice & Bob must have key
   Encryption randomized

2. Publicly known
   not proprietary
   don't implement your own

3. Cryptography is necessary
   but not sufficient
   - social eng.
   - software bugs
   - wrong implementations of crypto

One-Time Pad (OTP)

$m \in \{0,1\}^n$ Alice $\xrightarrow{c = m \oplus k}$ Bob

$k \in \{0,1\}^n$ Alice

$k \in \{0,1\}^n$ Bob

Alice:

m	0	1	0	0	1	⊕
k	1	0	1	0	0	
c	1	1	1	0	1	

Bob:

c	1	1	1	0	1 ⊕
k	1	0	1	0	0
m	0	1	0	0	1

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

$D(k,c) = c \oplus k$

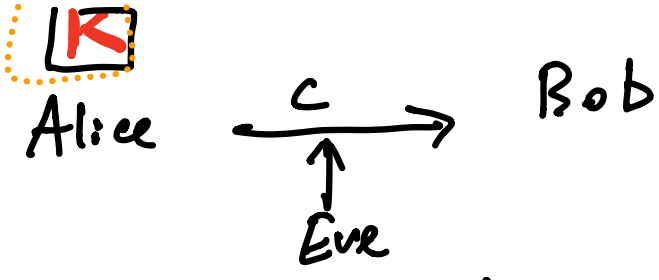
Correctness of OTP

$D(k, E(k,m)) = k \oplus E(k,m) = k \oplus (k \oplus m)$

$= m$ □

Perfect Secrecy

$\forall c : \forall m$ $\quad P_R[E(k,m) = c]$ is fixed – it doesn't depend on m



Eve sees c, she wants to learn some info about m.

Every m is equally likely.

$m_0 = 0000 \rightarrow c$

$m_1 = 0001 \rightarrow c$

$m_2 = 0010 \rightarrow c$

However powerful Eve is, she learns nothing about m

OTP is perfectly secure

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

$\forall c, \forall m$

How many keys k map $m \to c$?

$E(k,m) = m \oplus k' = c'$

$k = c \oplus m$

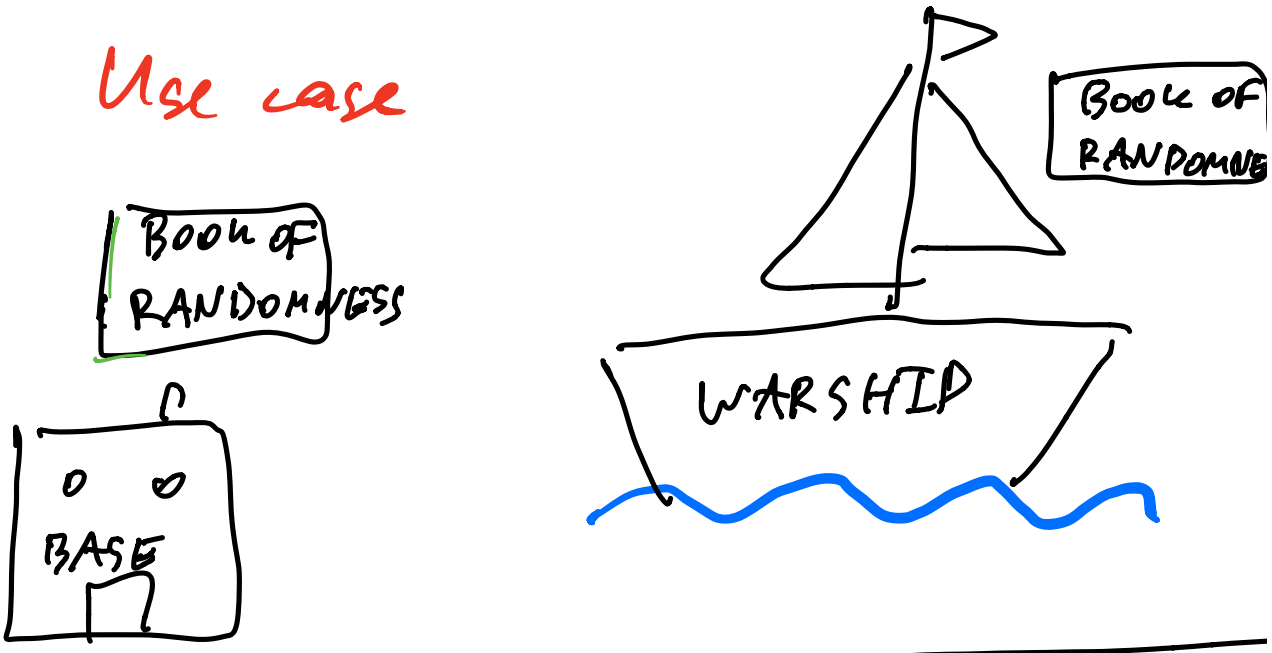
$P_{k}[E(k,m)=c] = \frac{1}{2^n}$ is

Fixed — doesn't depend on m. □

Key length = message length

IF we assume Alice & Bob can secretly share key of length n, can they can secretly communicate message m of length n?

Use case



ONE-TIME PAD can be used with fixed only ONCE

$$\text{Eve}\begin{cases} C_1 = m_1 \oplus k \\ C_2 = m_2 \oplus k \end{cases}$$

$$C_1 \oplus C_2 = m_1 \oplus m_2$$

Redundancy $m_1 \oplus m_2 \rightarrow m_1, m_2$

Venona Project

Shannon's Thm: $\forall$ perfectly secure ciphers, key length $\geq$ msg length

Stream Ciphers

A way to make OTP practical — publicly known PRGs

Pseudorandom Generators (PRG)

$$f: \{0,1\}^s \longrightarrow \{0,1\}^n$$

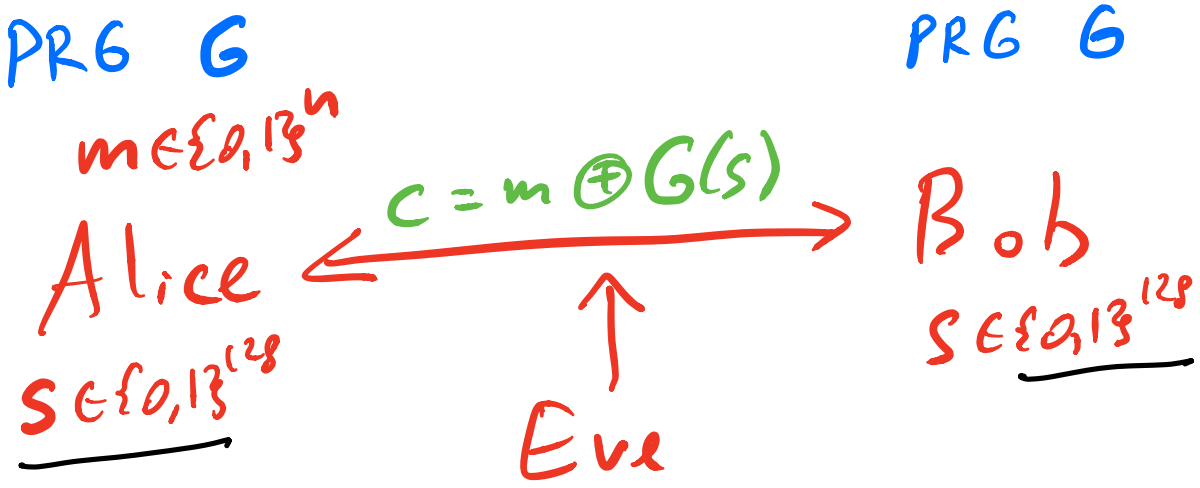
- $\{0,1\}^s$: SEED, $s \approx 128$
- $\{0,1\}^n$: pseudo-random OUTPUT, $n > 10^9$

Pseudo-random – for every efficient Eve, the output of PRG's looks random.

Efficient – poly time, i.e. runs $< 10^{30}$ steps

Eve sees $k \in \{0,1\}^n$, can't tell it apart from truly random.

(IF Eve could run in exp time, she would distinguish output of PRG from random)



$G(s) \in \{0,1\}^n$

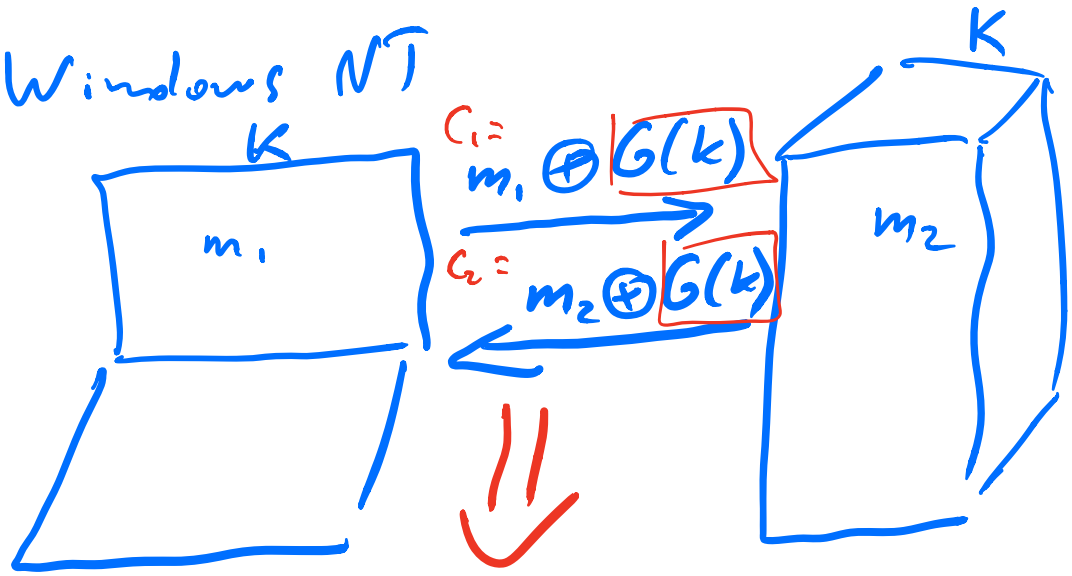
$c = m \oplus G(s)$ – Alice

Bob: $G(s) \oplus c = G(s) \oplus m \oplus G(s) = m$

Connectness

Security: efficient Alice can't decode it

Attacks on (bad implementations) of stream ciphers



$$C_1 \oplus C_2 = m_1 \oplus m_2$$

$$\Downarrow$$

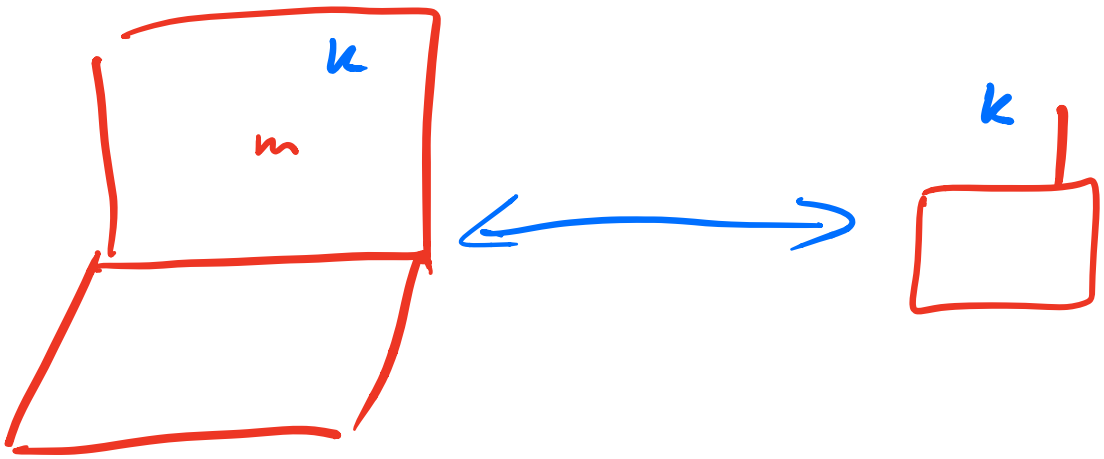
$$m_1, m_2$$

k_1, k_2 $\qquad$ k_1, k_2

$m_1 \oplus G(k_1)$ →

← $m_2 \oplus G(k_2)$

802.11b WEP



$m = m_1, m_2 \ldots m_n$

$m_1 \oplus G(k)$

$m_2 \oplus G(k)$ $\quad i \in \{0,1\}^{24}$

$m_1 \oplus G(k[1])$ →

$m_2 \oplus G(k2)$ →

$m_3 \oplus G(k3)$ →

$m_n \oplus G(k4)$ →

Power cycle

↓

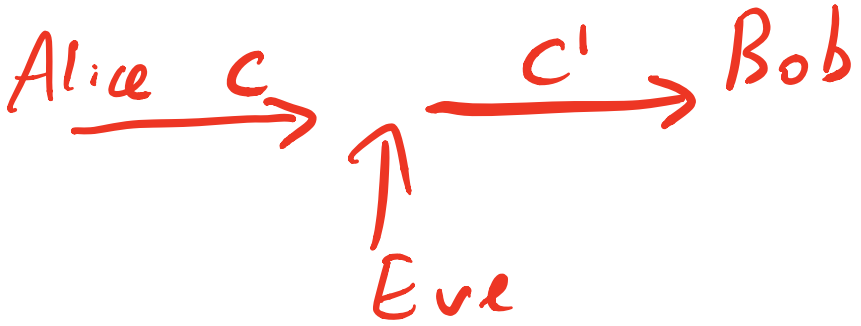
$i = 1$

After $2^{24} \approx 16M$ messages, you use the same / Later 40k messages

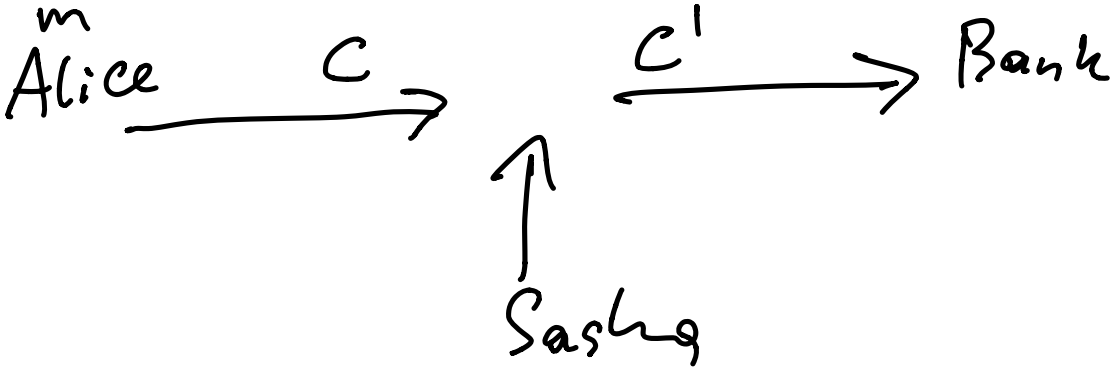
$G(k) \longrightarrow \{0,1\}^{109}$

$m \oplus G(k)$

Integrity



We'll see achieve integrity



m = Alice gets $100 ..... .

$c' = c \oplus x$

$x_1 = A \oplus S$
$x_2 = 1 \oplus a$
$x_3 = i \oplus s$
$x_4 = c \oplus h$
$x_5 = e \oplus a$

m = Alice gets $100 ~ ... - - .

$c' = c \oplus x$

$x_1 = A \oplus S$ $\quad x_6 = 0$

$x_2 = l \oplus a$ $\quad \vdots$

$x_3 = i \oplus s$

$x_4 = c \oplus h$ $\quad x_n = 0$

$x_5 = e \oplus a$

$c = m \oplus k$

Bob $c' \oplus k = m \oplus x =$

$=$ "Sasha gets $100 - - - "

Stream ciphers secure against ciphon-text attacks, we still want more: integrity