CSE 433S: Introduction to Computer Security

Cryptography Overview,
Classic Cipher, Stream Cipher

Washington University in St. Louis

Previously in 433S: Network Attacks

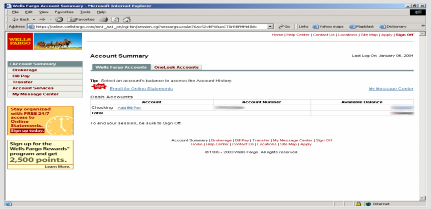
- Can you sniff packet in the network? Why or Why not?
- Can you spoof packet in the network? Why or Why not?
- What is smurf attack?
- What is TCP sync flood attack?
- Is increasing the buffer the right approach to defend against TCP sync flood?
- What connection information does an attack need to know to launch TCP hijacking attack?

Lecture outline for today

- Why do we need cryptography?
- What is cryptography?
- Classic Cipher
- Stream Cipher

Why do we need cryptography?

Secure communication
- Example



Wells Fargo Account Summary - Microsoft Internet Explorer

Address https://online.wellsfargo.com/mn1_aa1_on/cgi-bin/session.cgi?sessargs=coAn76axS2xltPX8uoCT8rRBfMMdJldx

Home | Help Center | Contact Us | Locations | Site Map | Apply | Sign Off

- Account Summary
- Brokerage
- Bill Pay
- Transfer
- Account Services
- My Message Center

Stay organized with FREE 24/7 access to Online Statements. Sign up today.

Sign up for the Wells Fargo Rewards® program and get 2,500 points. Learn More.

Account Summary

Last Log On: January 06, 2004

Wells Fargo Accounts | OneLook Accounts

Tip: Select an account's balance to access the Account History.

NEW Enroll for Online Statements

My Message Center

Cash Accounts

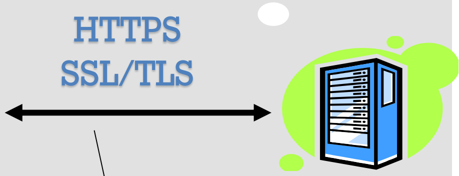
Account	Account Number	Available Balance
Checking Add Bill Pay	[redacted]	[redacted]
Total		[redacted]

To end your session, be sure to Sign Off.

Account Summary | Brokerage | Bill Pay | Transfer | My Message Center | Sign Off
Home | Help Center | Contact Us | Locations | Site Map | Apply

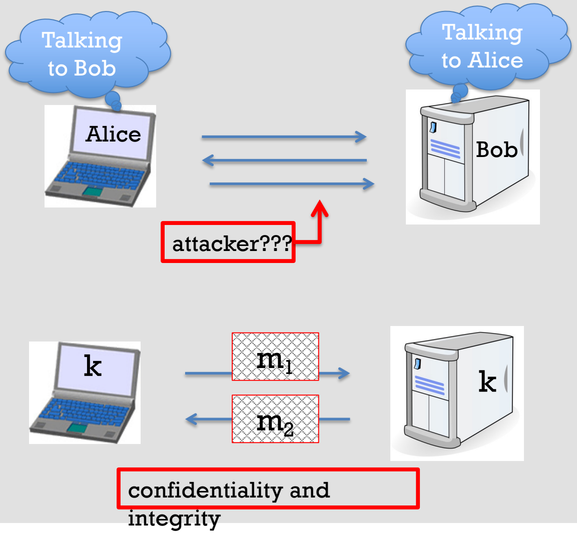
© 1995 - 2003 Wells Fargo. All rights reserved.

File Edit View Favorites Tools Help
Back Favorites
Go Links Yahoo maps Mapblast Dictionary
Internet



no eavesdropping
no tampering

Crypto core



Secret key establishment:

Secure communication:

confidentiality and integrity

Secure Sockets Layer / TLS

Two main parts

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

2. Record Layer: **Transmit data using shared secret key**

   Ensure confidentiality and integrity

Things to remember

- Cryptography is:
  - A tremendous tool
  - The basis for many security mechanisms
- Cryptography is not:
  - The solution to all security problems
  - Reliable unless implemented and used properly
  - Something you should try to invent yourself
    - many many examples of broken ad-hoc designs

A rigorous science

The three steps in cryptography:

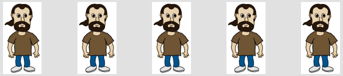
- Precisely specify threat model
- Propose a construction
- Prove that breaking construction under threat mode will solve an underlying hard problem

For the first half of the semester, we will focus on

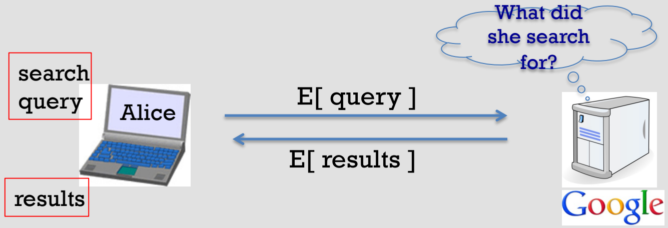
- Stream Cipher
- Symmetric Cryptography
- Asymmetric Cryptography
- Hash functions
- Authentication
- IPSec
- SSL/TLS
- PKI, HTTPS, E-mail
- Cryptocurrency

Advance Application of Cryptography that we will not cover in this course

- Elections
- Private auctions



- Privacy-preserving computation outsourcing



What did she search for?

search query

Alice

E[query]

E[results]

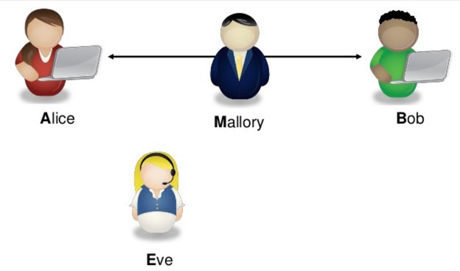
results

Review Questions (T or F)

- Cryptography is about obfuscating information, creating our own is a great way to hide it.
- Eve is usually entity initiating communication with Bob.
- Cryptographic implementation is easy, as long as the math is correct, the system will also perform correctly.

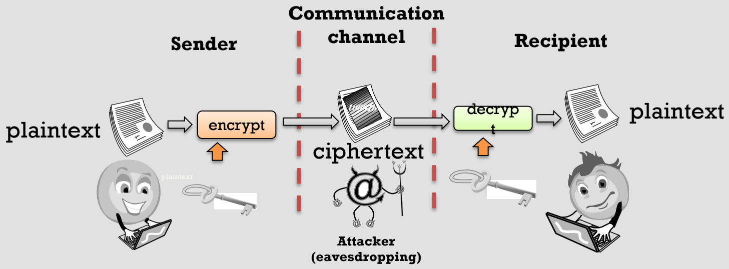
What is cryptography?

Background: common roles in cryptography



Overview: Encryption and Decryption

- The message M is called the **plaintext.**
- Alice will convert plaintext M to an encrypted form using an encryption algorithm E that outputs a **ciphertext C for M.**



Sender

Communication channel

Recipient

plaintext

encrypt

ciphertext

decryp t

plaintext

Attacker (eavesdropping)

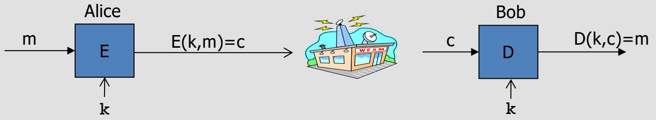
Background: cryptography goals

- Confidentiality:
  - Mallory and Eve cannot recover original message from ciphertext
- Integrity:
  - Mallory cannot modify message from Alice to Bob without detection by Bob

Overview: Cryptosystem components

1. The set of possible plaintexts
2. The set of possible ciphertexts
3. The set of encryption keys
4. The set of decryption keys
5. The correspondence between encryption keys and decryption keys
6. The encryption algorithm to use
7. The decryption algorithm to use

Building blocks: symmetric encryption



Alice

m

E

E(k,m)=c

k

Bob

c

D

D(k,c)=m

k

E, D: cipher k: secret key (e.g. 128 bits)

m, c: plaintext, ciphertext

Encryption algorithm is publicly known

- “security through obscurity” doesn’t work

Symmetric ciphers: definition

Def: a **cipher** defined over (K, M, C)

is a pair of “efficient” algs (***E***, ***D***) where

E: K x M → C

D: K x C → M

Correctness Property:

$$\forall m \in M, k \in K: D\big(k, E(k,m)\big) = m$$

- ***D*** and ***E*** are often efficient (polynomial time | concrete time)
- ***E*** is encryption, often randomized.
- ***D*** is decryption, always deterministic.

Threat models

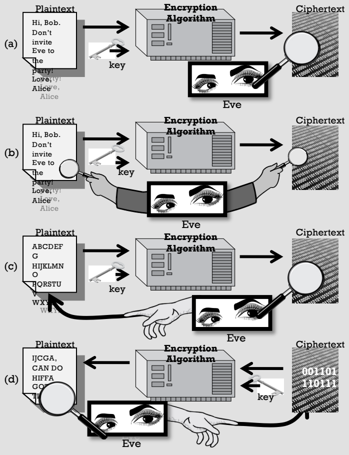
- Attacker may have:

a) collection of ciphertexts (ciphertext-only attack)

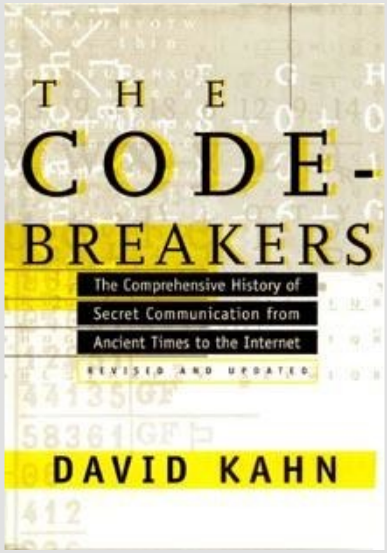
b) collection of plaintext/ciphertext pairs (known plaintext attack: KPA)

c) collection of plaintext/ciphertext pairs for plaintexts selected by the attacker (chosen plaintext attack: CPA)

d) collection of plaintext/ciphertext pairs for ciphertexts selected by the attacker (chosen ciphertext attack: CCA/CCA2)



Cryptography History



THE CODE-BREAKERS

The Comprehensive History of Secret Communication from Ancient Times to the Internet

REVISED AND UPDATED

DAVID KAHN

Caesar Cipher (no key, n letter shift)

- In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques.
- It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.

Substitution cipher

In cryptography, a substitution cipher is a method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system

`k :=`

What is the size of key space in the substitution cipher assuming 26 letters?

$|\mathcal{K}| = 26$

$|\mathcal{K}| = 26!$

$|\mathcal{K}| = 2^{26}$

$|\mathcal{K}| = 26^{2}$

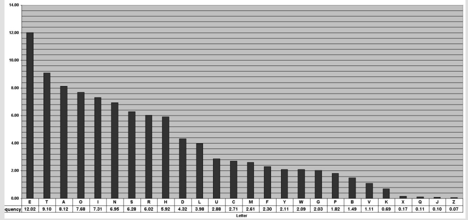
How to break a substitution cipher?

What is the most common letter in English text?

"X"
"L"
"E"
"H"

How to break a substitution cipher?

(1) Use frequency of English letters



(2) Use frequency of pairs of letters (digrams)

["th",100272945963],
["he",86697336727],
["in",68595215308],
["er",57754162106],
["an",55974567611],

An Example

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERV
NBCVBPCYYFVUFOFEIKNWFRFIKJNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHX
CYBOHOPYXPUBNCUBOYNRVNIWNCPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCB
BONCHRJZSFWNVRJRUBZRPCYZPUKBZPUNVPWPCYVFZIXUPUNFCPWRVNBCVB
RPYYNUNFCPWWJUKBYBIPOUZBCUIPOUNVNIPUBRNCHOPYXPUBNCUBOYNRVN
IWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZP
UNVR

B	36
N	34
U	33
P	32
C	26

→ E

→ T

→ A

N C	11
PU	10
UB	10
UN	9

→ IN

→ AT

digrams

UKB	6
RVN	6
FZI	4

→ THE

trigrams

2. Vigener cipher (16'th century, Rome)

k = C R Y P T O C R Y P T O C R Y P T

m = W H A T A N I C E D A Y T O D A Y

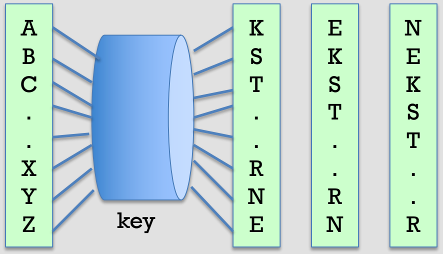
(+ mod 26)

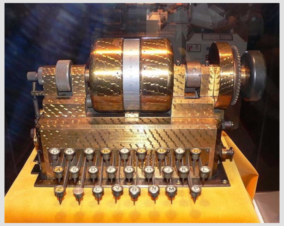
c = Z Z Z J U C L U D T U N W G C Q S

suppose most common = "H" ⟹ first letter of key = "H" – "E" = "C"

3. Rotor Machines (1870-1943)

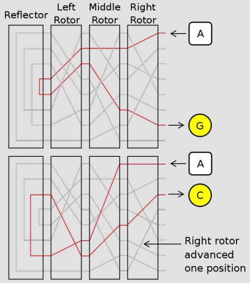
- Early example: the Hebern machine (single rotor)





Rotor Machines (cont.)

- Most famous: the Enigma (3-5 rotors)



# keys = $26^4 = 2^{18}$ (actually 2^{36} due to plugboard)

4. Data Encryption Standard (1974)

DES: # keys = 2^{56} , block size = 64 bits

Today: AES (2001), Salsa20 (2008) (and many others)

Review Questions

- What is the size of key space in the substitution cipher assuming 26 letters?
- Can you describe the process you will follow to crack a substitution cipher ? In your method to crack the cipher, which one(s) out of the three key cornerstones did you take advantage of?

Review on Discrete Probability

Discrete Probability Distribution

U: finite set (e.g. $U = \{0,1\}^n$)
Def: Probability distribution P over U is a function
$P: U \longrightarrow [0,1]$ such that

$$\sum_{x \in U} P(x) = 1$$

Examples:
Uniform distribution: for all $x \in U$: $P(x) = 1/|U|$

Point distribution at x_0: $P(x_0) = 1$, $\forall x \neq x_0$: $P(x) = 0$

Distribution vector: (P(000), P(001), P(010), … , P(111))

The uniform random variable

Let U be some set, e.g. $U = \{0,1\}^n$

We write $r \xleftarrow{R} U$ to denote a **uniform random variable** over U

for all $a \in U$: $\Pr[\, r = a \,] = 1/|U|$

(formally, r is the identity function: $r(x)=x$ for all $x \in U$)

Review: XOR

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

$$\begin{array}{r} 0\;1\;1\;0\;1\;1\;1 \\ \oplus \quad 1\;0\;1\;1\;0\;1\;0 \\ \hline \end{array}$$

An important property of XOR

Thm: Y a rand. var. over $\{0,1\}^n$,
X an indep. uniform var. on $\{0,1\}^n$
Then $Z := Y \oplus X$ is uniform var. on $\{0,1\}^n$

Proof: (for n=1) then use induction

P (Y = 0) = P_Y0, P (Y = 1) = P_Y1
P (x = 0) = P_X0, P (x =1) = P_X1

*P(Z=0) = P_Y0 * P_X0 + P_Y1*P_X1*

Since P_X0 = P_X1 = ½ due to uniform random

*P(Z=0) = (P_Y0+P_Y1) * ½ = ½*

Therefore Z is also uniformly random

Stream Ciphers

Symmetric Ciphers: definition

Def: a **cipher** defined over (K, M, C)

is a pair of “efficient” algs (***E***, ***D***) where
E: K x M → C
D: K x C →M

Correctness Property:

$$\forall m \in M, k \in K: D\big(k, E(k,m)\big) = m$$

- ***D*** and ***E*** are often efficient (polynomial time | concrete time)
- ***E*** is encryption, often randomized.
- ***D*** is decryption, always deterministic.

The One Time Pad (Vernam 1917)

First example of a "secure" cipher,
OTP: $E(k,m) = m \oplus k$, $D(k,c) = c \oplus k$

$M = C = \{0,1\}^n$, $K = \{0,1\}^n$

key = (random bit string as long the message)

The One Time Pad (Vernam 1917)

msg: 0 1 1 0 1 1 1
key: 1 0 1 1 0 1 0 $\oplus$

CT:

Discussion Question

- Given the message m and its ciphertext c, can you recover the key for OTP?

The One Time Pad (Vernam 1917)

Very fast enc/dec !!

Is the OTP secure? What is a secure cipher?

Information Theoretic Security (Shannon 1949)

Shannon's idea:

CT should reveal no "info" about PT under CT only attack

Def: A cipher ***(E,D)*** over (K,M,C) has **perfect secrecy** if

$\forall m_0, m_1 \in M \quad (|m_0| = |m_1|) \quad$ and $\quad \forall c \in C$

$$Pr[\, E(k,m_0)=c \,] \;=\; Pr[\, E(k,m_1)=c \,] \qquad \text{where } k \xleftarrow{R} K$$

Let $m \in \mathcal{M}$ and $c \in \mathcal{C}$.

How many OTP keys map $\boldsymbol{m}$ to $\boldsymbol{c}$?

None

1

2

Depends on $\boldsymbol{m}$

Lemma: OTP has perfect secrecy.

Proof:

assuming $k \xleftarrow{R} K$

$$\forall m, c \quad P[\, E(k,m) = c \,] = \frac{\#\text{ keys map } m \to c}{|K|}$$

$$\forall m, c \quad |\, k \in K \mid E(m,k) \,| = 1$$

$$\Rightarrow \forall m_0, m_1, c, \text{ st } |m_0| = |m_1|$$

$$Pr[\, E(k, m_0) = c \,] = 1/|K| \quad k \xleftarrow{R} K$$

$$Pr[\, E(k, m_1) = c \,] = 1/|K| \quad k \xleftarrow{R} K$$

$\Rightarrow$ OTP has perfect secrecy.

Problem solved ?

- OTP has perfect secrecy according to Shannon's theory, are we done ?

Stream Ciphers:
making OTP practical

idea: replace “random” key by “pseudorandom” key

Making OTP practical using a PRG: G: K ⟶ $\{0,1\}^n$

Stream cipher:

E(k,m) = m ⊕ G(k) ,   D(k,c) = c ⊕ G(k)

Question:
Can a stream cipher have perfect secrecy?

Yes, if the PRG is really “secure”

No, there are no ciphers with perfect secrecy

Yes, every cipher has perfect secrecy

No, since the key is shorter than the message

Stream Ciphers:
making OTP practical

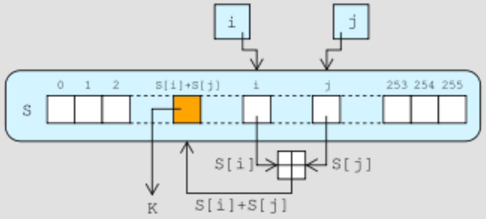
If stream ciphers has no perfect secrecy, then how do we argue about the security of stream cipher?

– Need a different definition of security

- Security will depend on specific PRG

A concrete example – RC4

- increments *i*
- looks up the *i*th element of S, S[*i*], and adds that to *j*
- exchanges the values of S[*i*] and S[*j*] then uses the sum S[*i*] + S[*j*] (modulo 256) as an index to fetch a third element of S (the keystream value K below)
- then bitwise exclusive ORed (XORed) with the next byte of the message to produce the next byte of either ciphertext or plaintext.



How do you show stream cipher is secure ?

A rigorous science

The three steps in cryptography:

- Precisely specify threat model
- Propose a construction
- Prove that breaking construction under threat mode will solve an underlying hard problem

Analysis for today

- Threat model: ciphertext-only attack
- Construction: rules of OTP, stream-cipher key generator, etc.
- Hard/impossible problem: differentiating between uniform-random outputs

- Note: other options exist for all these components!

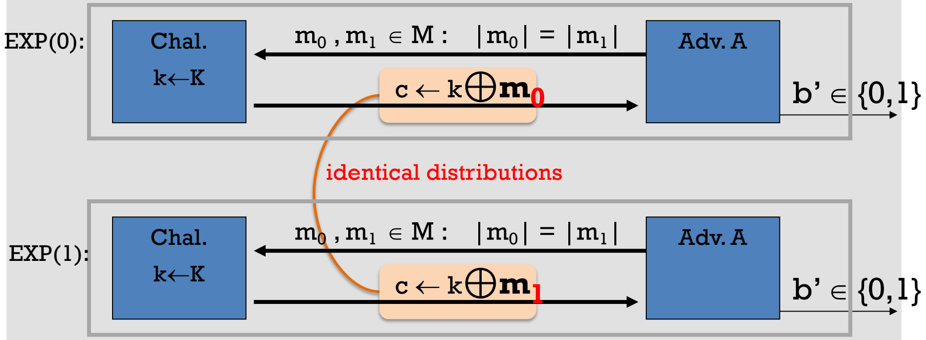
Semantic Security (one-time key)

Def: $\mathbb{E}$ is **semantically secure** if for all **efficient** A

$\mathrm{Adv}_{\mathrm{SS}}[A,\mathbb{E}]$ is negligible.

$\Rightarrow$ for all explicit m_0 , m_1 $\in$ M : $\{\ E(k,m_0)\ \} \approx_p \{\ E(k,m_1)\ \}$

OTP is semantically secure


EXP(0):
Chal.
k←K
$m_0, m_1 \in M: \; |m_0| = |m_1|$
Adv. A
$c \leftarrow k \oplus m_0$
$b' \in \{0,1\}$
identical distributions
EXP(1):
Chal.
k←K
$m_0, m_1 \in M: \; |m_0| = |m_1|$
Adv. A
$c \leftarrow k \oplus m_1$
$b' \in \{0,1\}$

For **all** A: $\mathrm{Adv}_{SS}[A, OTP] = \big| \Pr[\, A(k \oplus m_0) = 1 \,] - \Pr[\, A(k \oplus m_1) = 1 \,]$ 0

What happens when assumptions are violated – attack on stream cipher

Weak PRGs (do not use for crypto)

Kerberos v4 made this mistake

glibc random():

$r[i] \leftarrow (\, r[i-3] + r[i-31] \,) \;\%\; 2^{32}$

output $r[i] >> 1$

Attack 1: **two time** pad is insecure !!

Never use stream cipher key more than once !!

$C_1 \leftarrow m_1 \oplus \mathrm{PRG}(k)$

$C_2 \leftarrow m_2 \oplus \mathrm{PRG}(k)$

Eavesdropper does:

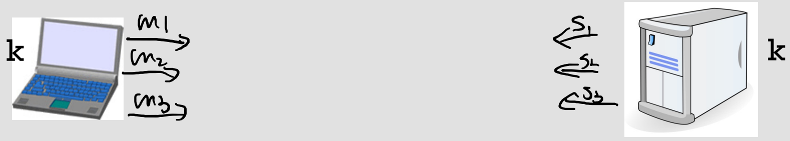
$C_1 \oplus C_2 \;\rightarrow\; m_1 \oplus m_2$

Enough redundancy in English and ASCII encoding that:

$m_1 \oplus m_2 \;\rightarrow\; m_1, \; m_2$

Real world examples

- Project Venona
- MS-PPTP (windows NT):



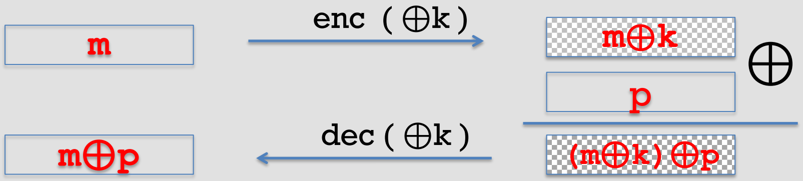
$[m_1 \| m_2 \| m_3 \ldots] \oplus PRG(k)$

$[s_1 \| s_2 \| s_3 \ldots] \oplus PRG(k)$.

Need different keys for C⟶S and S⟶C

one key for each direction.

Attack 2: no integrity (OTP is malleable)



Modifications to ciphertext are undetected and have **predictable** impact on plaintext

Attacks on Stream Cipher

- Examples of using the same stream twice
  - Project Verona(Russian Intelligence 1941)
  - WEP
  - Don’t use it twice, negotiate new key for every session (e.g. TLS)
- OTP is malleable
  - Add integrity check

Summary – Classic and Stream Cipher

- Caesar Cipher, Substitution Cipher
- Frequency attack
- Rotor Machine, Egnima Machine
- XOR with uniform random variable
- Perfect Secrecy - One time pad
- Attack on Stream Cipher
  - Two time pad
  - Integrity attack