Network Information Security

Lecture four: stream cipher

Rachel yuan

2019.9

1

Symmetric Ciphers: definition

Def: a **cipher** defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$

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

$E: \mathcal{K} \times \mathcal{M} \to \mathcal{C}$, $D: \mathcal{K} \times \mathcal{C} \to \mathcal{M}$

s.t. $\forall m \in \mathcal{M}, k \in \mathcal{K}: D(k, E(k, m)) = m$

Dan Boneh

2

Wrap up

- $(\mathcal{E}, \mathcal{D}, \mathcal{M}, \mathcal{K}, \mathcal{C})$ (密码系统五元组)
- Classical cipher
  - Substitution cipher
    - Monoalphabetic cipher — Caesar cipher
    - Polyalphabetic cipher — Vigenère cipher
- How to break?
  - Brute force
  - Frequency analysis

3

Vigenère Cipher exercise

Try to encode "UNDERATTACK" using the key CAR

message:	**U**	**N**	**D**	**E**	**R**	**A**	**T**	**T**	**A**	**C**	**K**
repeated keyword:	C	A	R	C	A	R	C	A	R	C	A
encoded message:	**W**	**N**									

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

4

Transposition Cipher (置换密码)

- Rearrange letters in plaintext to produce ciphertext
- Example: **Rail-Fence Cipher (栅栏密码)**
  - Plaintext is **HELLO WORLD**
  - Rearrange as
    HLOOL
    ELWRD
  - Ciphertext is **HLOOL ELWRD**
  - Question: `What is the key?`

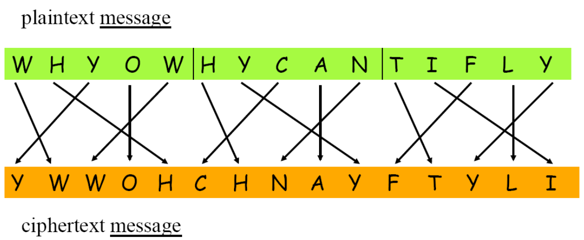
5

- Encode the phrase WE NEED YOUR HELP using the Rail Fence cipher.

6

Transposition cipher

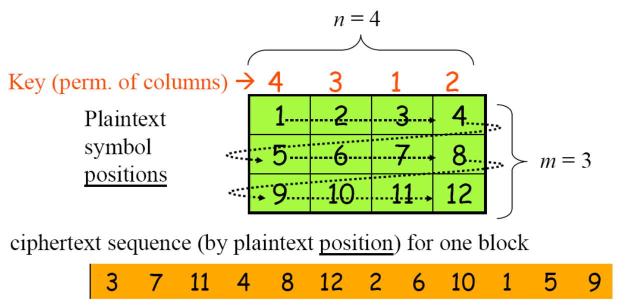
- Transposition cipher example #1:
  - Permute each successive block of 5 letters in the message according to position offset <+1, +3, -2, 0, -2>



7

Transposition cipher (cont'd)

- Transposition cipher example #2：
  - Arrange plaintext in blocks of n columns and m rows
  - Then permute columns in a block according to a key K



8

Transposition cipher (cont'd)

- A longer example: plaintext =
- "ATTACK POSTPONED UNTIL TWO AM"

Key:	4	3	1	2	5	7	6
plaintext	A	T	T	A	C	K	P
	O	S	T	P	O	N	E
	D	U	N	T	I	L	T
	W	O	A	M	X	Y	Z

ciphertext

TTNA APTM TSUO AODW COIX PETZ KNLY

9

Classical Cryptography（经典加密方法）

- Two basic types of classical ciphers
  - Transposition ciphers (置换密码)
  - Substitution ciphers (替换密码)
  - Combinations are called *product ciphers* (组合密码)

- Transposition cipher: rearranges the characters in the plaintext to form the ciphertext. The letters are not changed.
- Substitution cipher: change characters in the plaintext to produce the ciphertext.

10

outline

- One time pad (一次密码簿)
- Perfect secrecy – Shannon
- Stream cipher (流密码)

11

How to increase the secrecy of cipher?

Randomness(随机性)

12

One time pad

If the ... ng as
the me ... comes
kno... used

13

Vernam cipher

- AT&T公司的Gilbert Vernam在1917年发明的一种加密方案。

$$c_i = p_i \oplus k_i$$

$$p_i = c_i \oplus k_i$$

- Use a very long but repeating keyword.

14

Truth table of XOR

x⊕y	x	y

15

OTP：one time pad

- Joseph Mauborgne proposed an improvement on Vernam cipher.
  - Key is as long as the message.
  - Key is only used one time.

video One time pad

16

The One Time Pad (Vernam 1917)

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

First example of a "secure" cipher

$k \in \mathcal{K}$

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

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

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

key = (random bit string as long the message)

Dan Boneh

17

The One Time Pad (Vernam 1917)

$D(k, E(k,m)) = D(k, k \oplus m) = (k \oplus k) \oplus m = 0 \oplus m = m$

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

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

msg: 0 1 1 0 1 1 1

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

CT:

Try to verify the consistency of One Time Pad.

18

One time pad

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

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

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

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

19

Perfect secrecy

Def: A cipher (***E***, ***D***) over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ has **perfect secrecy** if

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

$\boxed{\Pr[\mathbf{E}(k, m_0) = c] = \Pr[\mathbf{E}(k, m_1) = c]}$ where $k \leftarrow \mathcal{K}$

Basic idea: Cipher text (CT) should reveal(揭示) no information about plain text (PT).

如果我是一个攻击者，我截取了一段密文，c，这段密文 c 对应的明文是 m_0 的概率与对应的明文是 m_1 的概率相同。

唯密文攻击

20

One time pad has perfect secrecy

To proof $Pr[\, \boldsymbol{E(k, m_0) = c} \,] = Pr[\, \boldsymbol{E(k, m_1) = c} \,]$

$\forall$m,c:

$Pr[\boldsymbol{E(k,m) = c}]$ = (#keys k∈K s.t. E(k,m)=c)/|K|

So, if #{k∈K s.t. E(k,m)=c} = const,

We can proof cipher has perfect secrecy.

21

One time pad has perfect secrecy

For OTP:

$\forall$ m, c:

If E(k, m) = c

→ k ⊕ m = c

→ k = m ⊕ c

→ # (k∈K s.t. E(k,m)=c) = 1

→ OTP has perfect secrecy.■

22

单选题 1分 设置

You are given a message (*m*) and its OTP encryption (*c*).

Can you compute the OTP key from *m* and *c* ?

- A No, I cannot compute the key.
- B Yes, the key is $k = m \oplus c$.
- C I can only compute half the bits of the key.
- D Yes, the key is $k = m \oplus m$.

提交

23

Drawbacks of OTP

- **Truly Random**
- **As long as the message**
- **Secure exchange of OTP**
- **One time only use of the key**

24

The bad news …

Thm: perfect secrecy $\Rightarrow$ $|\mathcal{K}| \geq |\mathcal{M}|$

25

To make OTP practical:

Stream Cipher

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

26

Stream Ciphers: making OTP practical

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

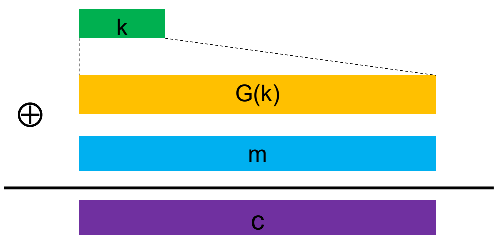
PRG: Pseudo Random Generator is a function, G

$$G: \{0, 1\}^s \rightarrow \underbrace{\{0,1\}^n}_{\textbf{Seed space}}, \quad n >> s$$

Efficiently deterministic algorithm

27

Stream Ciphers: making OTP practical



$c = E(k, m) := m \oplus G(k)$

$d = E(k, c) := c \oplus G(k)$

28

单选题 1分

设置

Can a stream cipher have perfect secrecy?

- A Yes, if the PRG is really “secure”
- B No, there are no ciphers with perfect secrecy
- C Yes, every cipher has perfect secrecy
- D No, since the key is shorter than the message

提交

29

Attacks on OTP and stream ciphers

30

Attack 1: two time pad is insecure !!

Never use stream cipher key more than once !!

$$C_1 \leftarrow m_1 \oplus PRG(k)$$
$$C_2 \leftarrow m_2 \oplus PRG(k)$$

Eavesdropper does:

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

Enough redundancy in English and ASCII encoding that:

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

31

Real world examples

- Project Venona
  - 1941 to 1946, decrypted about 3000 messages
- MS-PPTP (windows NT, point to point transfer protocol):

$[m_1||m_2||m_3] \oplus G(k)$ $[s_1||s_2||s_3] \oplus G(k)$

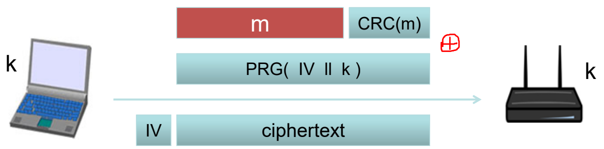
Need different keys for C→S and S→C

The shared key is actually a pair of keys: (Kc→s and Ks→c)
Both sides have these pair of keys.

32

Real world examples

802.11b WEP:



Length of IV: 24 bits

- Repeated IV after $2^{24} \approx$ 16M frames
- On some 802.11 cards: IV resets to 0 after power cycle

33

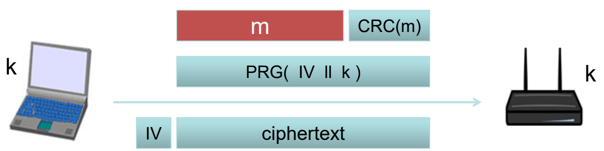
- 假设一个繁忙的**AP**（无线访问点），以**11Mbps**的速度发送大小为**1500bytes**的包，大约多长时间**IV**会耗光？

1500*8/(11*10^6)*2^24 = 18000秒，约为5 hours

34

Avoid related keys

802.11b WEP:



key for frame #1: (1 ll k)

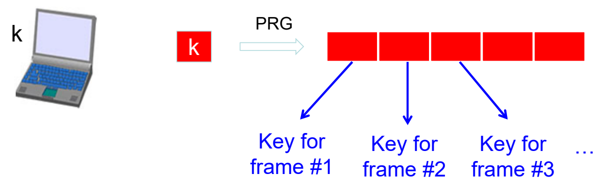
key for frame #2: (2 ll k)

⋮

FMS 2001 → can recover k after 10^6 frames, recent attacks ≈ 40,000 frames

35

A better construction

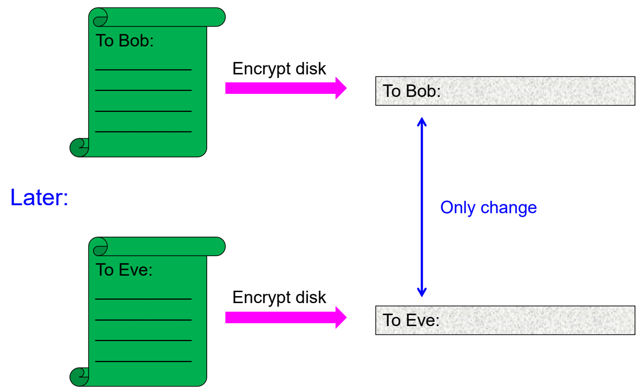


⇒ now each frame has a pseudorandom key

better solution: use stronger encryption method (as in WPA2)

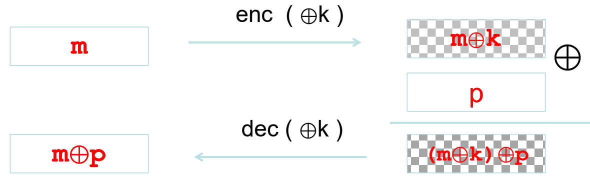
36

Yet another example: disk encryption



37

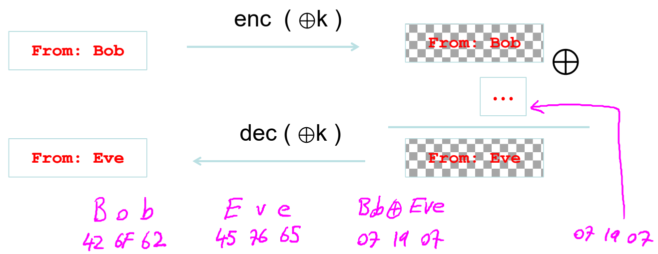
Attack 2: no integrity (OTP is malleable)



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

38

Attack 2: no integrity (OTP is malleable)



Modifications to ciphertext are undetected and have predictable impact on plaintext

39

Real world stream ciphers

40

RC4 stands for the fourth cipher designed by Ron Rivest (Rivest Cipher 4).

41