PESU Center for Information Security, Forensics and Cyber Resilience

Welcome to

PES University

Ring Road Campus, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

APPLIED CRYPTOGRAPHY

Lecture 10

Perfect secrecy limitations

Can it be achieved!!!

Disadvantages

- Distribution of the key was a challenge
- Adding numbers to the plaintext manually, is a time-consuming task. It is therefore sometimes thought that OTPs are no longer considered practical

Using same key twice

- If $c1= K \oplus m1$
- $C2= k\oplus m2$
- Then $c1\oplus c2= (k\oplus m1)\oplus(k\oplus m2)=m1\oplus m2$
- This leaks information about m1 and m2
- If $m1 \oplus m2 = 0$ shows that $m1=m2$
- If $m1\oplus m2=1$ shows $m1 != m2$
- Using frequency analyser they can decrypt the message

Same key more than once???

Hex	Dec	Char	Hex	Dec	Char	Hex	Dec	Char
0x20	32	Space	0x40	64	@	0x60	96	`
0x21	33	!	0x41	65	A	0x61	97	a
0x22	34	"	0x42	66	B	0x62	98	b
0x23	35	#	0x43	67	C	0x63	99	c
0x24	36	$	0x44	68	D	0x64	100	d
0x25	37	%	0x45	69	E	0x65	101	e
0x26	38	&	0x46	70	F	0x66	102	f
0x27	39	'	0x47	71	G	0x67	103	g
0x28	40	(	0x48	72	H	0x68	104	h
0x29	41	)	0x49	73	I	0x69	105	i
0x2A	42	*	0x4A	74	J	0x6A	106	j
0x2B	43	+	0x4B	75	K	0x6B	107	k
0x2C	44	,	0x4C	76	L	0x6C	108	l
0x2D	45	-	0x4D	77	M	0x6D	109	m
0x2E	46	.	0x4E	78	N	0x6E	110	n
0x2F	47	/	0x4F	79	O	0x6F	111	o
0x30	48	0	0x50	80	P	0x70	112	p
0x31	49	1	0x51	81	Q	0x71	113	q
0x32	50	2	0x52	82	R	0x72	114	r
0x33	51	3	0x53	83	S	0x73	115	s
0x34	52	4	0x54	84	T	0x74	116	t
0x35	53	5	0x55	85	U	0x75	117	u
0x36	54	6	0x56	86	V	0x76	118	v
0x37	55	7	0x57	87	W	0x77	119	w
0x38	56	8	0x58	88	X	0x78	120	x
0x39	57	9	0x59	89	Y	0x79	121	y
0x3A	58	:	0x5A	90	Z	0x7A	122	z
0x3B	59	;	0x5B	91	[	0x7B	123	{
0x3C	60	<	0x5C	92	\	0x7C	124	|
0x3D	61	=	0x5D	93	]	0x7D	125	}
0x3E	62	>	0x5E	94	^	0x7E	126	~
0x3F	63	?	0x5F	95	_	0x7F	127	DEL

- Letters all begin with 01…
- The space character begins with 00…
- XOR of two letters gives 00…
- XOR of letter and space gives 01…
- Easy to identify XOR of letter and space!

The Binary Version of One-Time Pad

Plaintext space = Ciphtertext space =

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

Key is chosen randomly

For example:

- Plaintext is 11011011
- Key is 01101001
- Then ciphertext is 10110010

Bit Operators

- Bit AND

$0 \wedge 0 = 0$ $0 \wedge 1 = 0$ $1 \wedge 0 = 0$ $1 \wedge 1 = 1$

- Bit OR

$0 \vee 0 = 0$ $0 \vee 1 = 1$ $1 \vee 0 = 1$ $1 \vee 1 = 1$

- Addition mod 2 (also known as Bit XOR)

$0 \oplus 0 = 0$ $0 \oplus 1 = 1$ $1 \oplus 0 = 1$ $1 \oplus 1 = 0$

  - 1's compliment
  - Left shift <<
  - Right shift >>
- Can we use operators other than Bit XOR for binary version of One-Time Pad?

Bitwise Operators - Examples

```
11010011
&
10001100
------------
10000000
```

```
11010011
|
10001100
------------
11011111
```

```
11010011
^
10001100
------------
01011111
```

```
~11010011
------------
 00101100
```

```
11010011>>3
------------
 00011010
```

```
11010011<<3
------------
 10011000
```

Key Randomness in One-Time Pad

- One-Time Pad uses a very long key, what if the key is not chosen randomly, instead, texts from, e.g., a book are used as keys.
  - this is not One-Time Pad anymore
  - this does not have perfect secrecy
  - this can be broken
  - How?
- The key in One-Time Pad should never be reused.
  - If it is reused, it is Two-Time Pad, and is insecure!
  - Why?

Usage of One-Time Pad

- To use one-time pad, one must have keys as long as the messages.
- To send messages totaling certain size, sender and receiver must agree on a shared secret key of that size.
  - typically by sending the key over a secure channel
- This is difficult to do in practice.
- Can’t one use the channel for send the key to send the messages instead?
- Why is OTP still useful, even though difficult to use?

Usage of One-Time Pad

- The channel for distributing keys may exist at a different time from when one has messages to send.

- The channel for distributing keys may have the property that keys can be leaked, but such leakage will be detected
  - Such as in Quantum cryptography

Summary

- Cryptology
  - Cryptography
  - Cryptanalysis
- Classical cryptography
  - Substitution ciphers
  - Transposition ciphers
- Steganography
- Cryptographic attack
- Probability and Shannon's theorem
- Perfect secret system

Next Class

- ☞ Mandatory reading for the next class
  - ☞ https://ieeexplore.ieee.org/document/7562224

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU ISFCR | PESU Center for Information Security, Forensics and Cyber Resilience

PESU IoT | PESU Center for Internet of Things