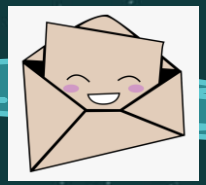
Cryptography & Steganography

Information Security – Lecture 03

Aadil Zia Khan

Alice, Bob, and the Eavesdropper (Eve)



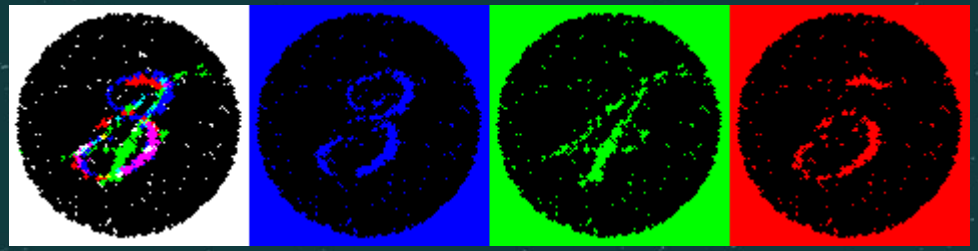
Confidentiality of Stored/Transmitted Data

- Good guys: Alice and Bob
- Eavesdropper/Adversary: Eve

- How can we prevent Eve from reading the exchanges between Alice and Bob???

Solution 1: Steganography

- Steganography is the practice of hiding a message within another message
  - Eve would not be aware of the existence of the hidden message



Same image under different lights

Solution 1: Steganography

- Take any data file
  - E.g., an image which wouldn't alert Eve

Solution 1: Steganography

- Edit the data file – replace some bytes with the message that you want to hide
  - You can write a short program
  - But you “love” programming - so let’s use a hex editor instead ☺

File Edit Search View Analysis Tools Window Help

16 | Windows (ANSI) | hex

WindsofDune-steg.jpg

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
0002FF30   DD 33 55 E4 B6 F9 B2 2A DA 9C 8A 08 A8 52 68 76  Ý3Uä¶ù²*ÚœŠ.¨Rhv
0002FF40   18 89 81 4B CD 49 DA 9A 69 0C AD 2F 4A A1 72 3F  .‰.KÍIÚši../J¡r?
0002FF50   8A B4 65 19 AA 52 28 C1 15 AD 36 44 89 EC E5 0C  Š´e.ªR(Á..6D‰ìå.
0002FF60   83 D6 AD AB 71 59 36 47 6B 10 2B 49 4D 4D 45 66  ƒÖ.«qY6Gk.+IMMEf
0002FF70   38 3D 09 F7 71 48 0E 7A D2 25 2D 66 50 D7 5C F3  8=.÷qH.zÒ%-fP×\ó
0002FF80   54 A5 8B 71 AB E7 A5 57 71 55 07 A8 99 15 BC 9B  T¥‹q«ç¥WqU.¨™.¼›
0002FF90   0E D3 56 D4 D5 19 38 E6 A7 B7 72 C3 9A B9 2E A0  .ÓVÔÕ.8æ§·rÃš¹.
0002FFA0   BB 16 29 A5 45 19 A4 A8 28 85 85 42 E8 09 CD 59  ».)¥E.¤¨(……Bè.ÍY
0002FFB0   61 50 48 31 56 89 21 F3 59 38 A1 26 CF 5A 46 19  aPH1V‰!óY8¡&ÏZF.
0002FFC0   A8 87 5A D1 2B 8A F6 2C 0B 84 FE 2A 98 CC 98 05  ¨‡ZÑ+Šö,.„þ*˜Ì˜.
0002FFD0   07 15 98 D4 8B 23 0E 86 9F 22 12 99 A8 26 19 C0  ..˜Ô‹#.†Ÿ".™¨&.À
0002FFE0   A7 86 E7 9A CF 8D C9 E4 D5 AD C4 8E 69 38 96 99  §†çšÏ.ÉäÕ.ÄŽi8–™
0002FFF0   65 E3 DA 37 29 A5 8A F0 FD C6 A6 C2 32 9C F6 AB  eãÚ7)¥ŠðýÆ¦Â2œö«
00030000   4C 45 54 27 53 20 57 41 54 43 48 20 44 55 4E 45  LET'S WATCH DUNE
00030010   9D 75 A9 27 96 72 39 A8 E1 72 09 5E D5 0E AD 0A  .u©'–r9¨ár.^Õ...
00030020   A2 6E 1D 48 A9 8A 4D EA 26 CE 6A F6 7F 3D C9 E9  ¢n.H©ŠMê&Îjö.=Éé
00030030   55 F3 8E 94 E9 8E 58 D4 5D 2B D0 4B 43 8A 4E EC  UóŽ”éŽXÔ]+ÐKCŠNì
00030040   76 7D 68 C8 A6 06 26 8C D5 08 93 E9 57 B4 E9 42  v}hÈ¦.&ŒÕ.“éW´éB
00030050   1C 35 67 8A 7E E2 39 15 32 57 45 C5 D9 DC E9 E3  .5gŠ~â9.2WEÅÙÜéã
00030060   BA 0B 8C 74 AB 5E 60 C6 6B 07 4E 9D 9B 83 5A A1  º.Œt«^`Æk.N.›ƒZ¡
00030070   8E DA E2 9C 52 67 5C 5D D1 69 79 39 A5 23 27 26  ŽÚâœRg\]Ñiy9¥#'&
00030080   A3 53 F2 D4 8A 72 2B 21 91 49 97 E9 50 48 A5 B8  £SòÔŠr+!'I—éPH¥¸
00030090   35 6A 41 81 C5 46 C3 BD 52 62 65 68 C9 84 FB 55  5jA.ÅFÃ½RbehÉ„ûU
000300A0   E5 70 E3 22 AB 48 03 0E 6A 3B 79 08 6D BD A9 BD  åpã"«H..j;y.m½©½
000300B0   55 FA 8B 62 D4 82 A0 63 B7 9A 9A 43 C5 57 7A 94  Uú‹bÔ‚ c·šš CÅWz”
000300C0   53 27 52 08 CD 3B A0 AA C8 C7 A5 4C 0E 69 30 25  S'R.Í; ªÈÇ¥L.i0%
000300D0   04 1A 5C 0A 8D 0D 3B 3C D4 81 14 90 F7 AA 53 27  ..\...;<Ô...÷ªS'
000300E0   35 A8 7A 55 69 94 1A A8 C8 4D 18 B7 16 CA FC 8E  5¨zUi”.¨ÈM.·.Êü Ž
000300F0   0D 36 D6 E6 5B 63 86 E4 53 AE D8 A3 F1 53 C4 A2  .6Öæ[c†äS®Ø£ñSÄ¢
00030100   45 F9 AB A6 FA 59 EA 9F E0 67 6D 6E B4 6B F1 34  Eù«¦úYêŸàgmn´kñ4
00030110   AD EE 84 A3 8A B0 AD 9A C1 04 C2 FF 00 25 6B 5B  .î„£Š°.šÁ.Âÿ.%k[
00030120   C8 58 02 6B 9E 71 B1 A4 5D C9 2E 20 12 0A CF 9E  ÈX.kžq±¤]É. ..Ïž
00030130   07 8C 65 4D 69 93 4D 60 08 E6 94 64 D0 34 51 87  .ŒeMi“M`.æ”dÐ4Q‡
00030140   50 DA 02 BF 5A B8 B3 87 1C 1A A7 71 02 13 D2 B3  PÚ.¿Z¸³‡..§q..Ò³
00030150   4C 8D 13 E1 49 C5 68 A0 A5 B6 82 BD B4 DC E8 96  L..áIÅh ¥¶‚½´Üè–
00030160   40 DC 53 24 80 35 51 B6 9D CD 68 29 2C 39 AC 9E  @ÜS$€5Q¶.Íh),9¬ž
00030170   8C A3 3E EB 4F 0D CA F0 6A BA 3C D6 FC 1E 95 B2  Œ£>ëO.Êðjº<Öü.•²
00030180   06 6A 39 63 53 DA AD 4F A3 D5 12 E3 D7 62 AD BE  .j9cSÚ.O£Õ.ã×b.¾
```

Special editors

Data inspector

Binary (8 bit)		11000001
Int8	go to:	-63
UInt8	go to:	193
Int16	go to:	-21823
UInt16	go to:	43713
Int24	go to:	-4740415
UInt24	go to:	12036801
Int32	go to:	381135553
UInt32	go to:	381135553
Int64	go to:	5428662637585476289
UInt64	go to:	5428662637585476289
LEB128	go to:	47043905
ULEB128	go to:	47043905
AnsiChar / char8_t		Á
WideChar / char16_t		c▯
UTF-8 code point		Overlong encoding (U+006A)
Single (float32)		2.96730054150787E-25
Double (float64)		8.61416132128177E54
OLETIME		Invalid
FILETIME		Invalid
DOS date		6/1/2065
DOS time		9:22:02 PM
DOS time & date		5/23/1991 9:22:02 PM
time_t (32 bit)		1/29/1982 6:59:13 AM
time_t (64 bit)		Invalid
GUID		{16B7AAC1-7BE8-4B56-9304-9F
Disassembly (x86-16)		sbr word [bp+si+$000016B7], bx

Byte order

(•) Little endian ( ) Big endian

[ ] Hexadecimal basis (for integral numbers)

Offset(h): 302DF

Overwrite

Solution 1: Steganography

- If there are many characters that you need to insert
  - Spread them all over the file so that the image quality doesn't suffer

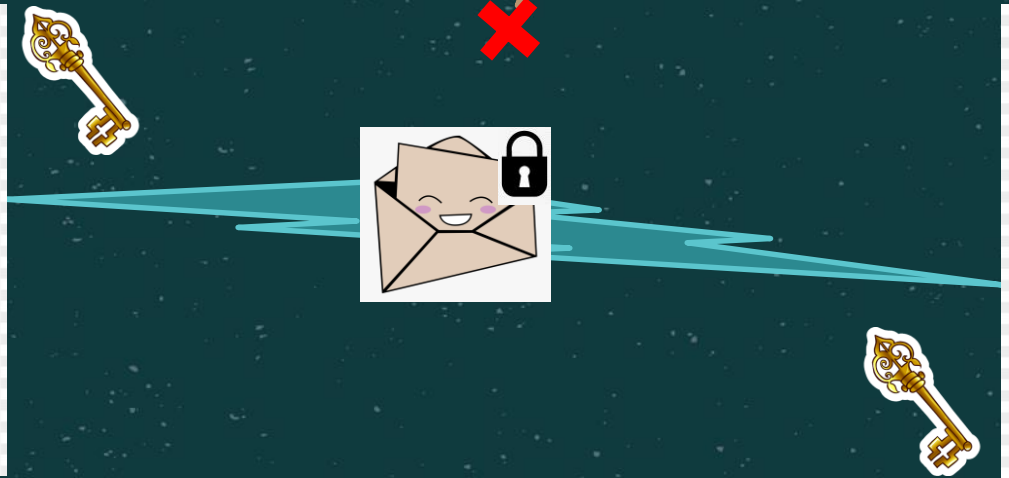
Solution 2: Encryption

- Do not hide the message – instead jumble it up so that no one other than Alice and Bob can understand it

Solution 2: Encryption

- Plaintext
  - The message that Alice and Bob don't want Eve to access
- Ciphertext
  - Jumbled up message which only those can un-jumble who possess the key
- Encryption/Decryption Algorithm (a.k.a the Cipher)
  - The steps taken to jumble up the plaintext or un-jumble the ciphertext
- Key
  - The secret value needed for encryption/decryption

Alice, Bob, and Eve



Solution 2: Encryption

- No need to keep the algorithm secret; we need to keep only the key secret
  - It is impractical to decrypt a message on the basis of the ciphertext plus knowledge of the encryption/decryption algorithm
- Why do we keep the algorithm open?
  - Because of the “Open Design” principle – if everybody knows the algorithm, they can identify weaknesses and thus help make it more secure

Cryptography

- Cryptography is about constructing and analyzing algorithms and protocols that prevent unauthorized people from reading messages

- Different from Steganography
  - Existence of the message is not hidden – the message is made unreadable

Cryptography - Classification

- Type of operation used
  - Substitution (each element in the plaintext is replaced with another element) **vs** Transposition (each element in the plaintext is rearranged)
- Number of keys used
  - Symmetric encryption (one secret key) **vs** Public-key encryption (one secret key and one know key)
- Processing method
  - Block cipher (plaintext processed in blocks) **vs** Stream cipher (plaintext processed one element at a time)

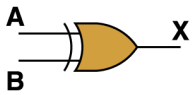
Using XoR for Encryption

XOR gate produces 0 if its inputs are the same, and a 1 otherwise

Boolean Expression

$X = A \oplus B$

Logic Diagram Symbol



Truth Table

A	B	X
0	0	0
0	1	1
1	0	1
1	1	0

USING EXCLUSIVE OR (XOR) IN CRYPTOGRAPHY

XOR LOGIC

XOR Symbol ⊕

0 XOR 0 = 0 Same Bits
1 XOR 1 = 0 Same Bits
1 XOR 0 = 1 Different Bits
0 XOR 1 = 1 Different Bits

ENCRYPT

```
  00110101  Plaintext
⊕ 11100011  Secret Key
= 11010110  Ciphertext
```

DECRYPT

```
  11010110  Ciphertext
⊖ 11100011  Secret Key
- 00110101  Plaintext
```

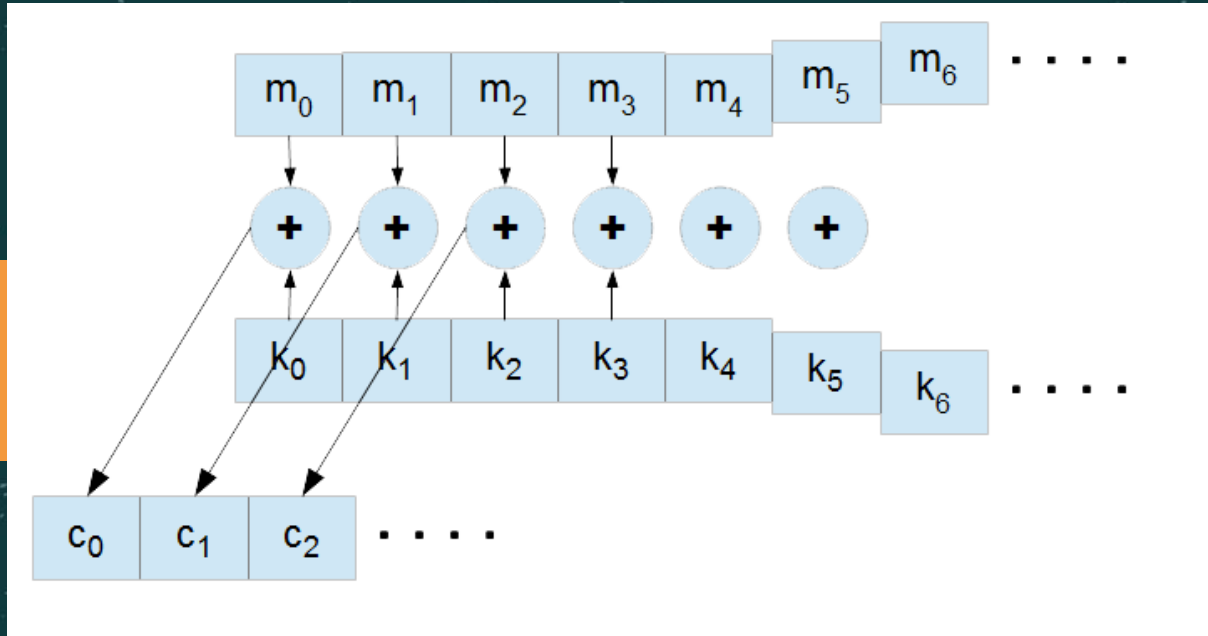
A Simple (yet most powerful) Cipher: One-Time Pad (OTP)

- Invented in 1917 by Gilbert Vernam, an engineer at AT&T Corporation in the USA
- Message (plaintext), Key, and Ciphertext have the same length
- Key is also called pad – random and known only to Alice and Bob
  - Was used by spies – written on a pad and discarded after use
  - Or the spy could use some agreed upon pages of an actual book as the key
- All bits of the plaintext and the key are XoR-ed to get the ciphertext
  - All bits of the ciphertext and the key are XoR-ed to get the plaintext

A Simple (yet most powerful) Cipher: One-Time Pad (OTP)

m_i XOR k_i = c_i

c_i XOR k_i = m_i



A Simple (yet most powerful) Cipher: One-Time Pad (OTP)

- Do you see any problems?

1. It is difficult to use
   - Requires the users to generate large secrets, share them, still keep them secret, and prevent reuse
2. It does not provide
   - Authentication of message (who sent it)
   - Protection against modification (did Eve change it)

A Simple (yet most powerful) Cipher: One-Time Pad (OTP)

- Sharing OTP between multiple people
  - OTP allows sharing the secret key among a number of people - each person will know only one subkey
  - Plaintext will be encrypted by XoR-ing it with each key one after the other
  - Encrypted text can be decoded by XoR-ing all three subkeys with the ciphertext one by one

Let's Try It Out!!!

https://www.boxentriq.com/code-breaking/one-time-pad

http://rumkin.com/tools/cipher/otp.php

Which one is better?

- The first one because it removes the space characters and converts each character to uppercase
- Because of space it becomes easy to identify/infer words like “the”, “is”, “an” in the ciphertext – this information together with the ciphertext can be used to determine the key
- (*more on this later*)