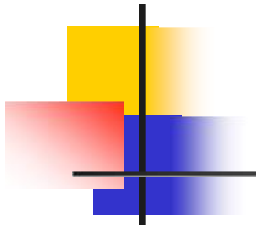
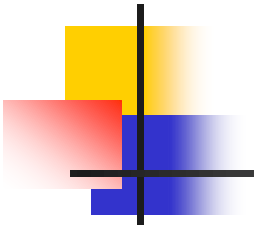


CSE 465
Information Assurance and Security

Cryptography and Steganography

Professor Stephen S. Yau



Cryptography

- In Greek means ***"secret writing"***
- An outsider (interceptor/intruder/adversary) can make following threats:
  - Block message (affecting availability)
  - Intercept message (affecting secrecy)
  - Modify message (affecting integrity)
  - Fabricate message (affecting integrity)
- The fundamental technique to counter these threats

Cryptography (cont.)

- ***Cryptography: Study*** of ***mathematical techniques*** related to **certain aspects of information security**, such as confidentiality, data integrity, entity authentication, and data origin authentication.
  - The basic component of cryptography is a ***cryptosystem***
- ***Cryptographer: Person*** working for ***legitimate*** sender or receiver. A cryptographer will use cryptography to convert plaintext into ciphertext.
- ***Cryptanalyst*: *Person*** working for ***unauthorized*** interceptor. A cryptanalyst will use cryptanalysis to attempt to turn ciphertext back into plaintext.
- ***Cryptology: Study*** of ***encryption and decryption***, including cryptography and cryptanalysis.

Cryptosystem

- *A **cryptosystem*** is a 5-tuple (E, D, M, K, C), where M is the set of ***plaintexts***, K is the set of ***keys***, C is the set of ***ciphertexts***, E: $M \times K \rightarrow C$ is the set of ***encipher*** (***encryption***) functions, and D: $C \times K \rightarrow M$ is the set of ***deciphering*** (***decryption***) functions.
  - Plaintext M: set of messages in original form
  - Ciphertext C: set of messages in encrypted form

Types of Cryptosystems

- ***Symmetric*** cryptosystems (also called ***single-key*** cryptosystems) are ***classical cryptosystems***:

  $M = D(K, E(K, M))$

  - The encryption key and decryption key are the same.
- ***Asymmetric*** cryptosystems:

  $M = D(K_d, E(K_e, M))$

  - K_d is the decryption key and K_e is the encryption key
  - $K_d \neq K_e$

Computational Security

- An encryption scheme is ***computationally secure*** if it takes ***exponentially long time*** to break the ciphertext.
- ***Lifetime*** of a cryptosystem: The minimum time for unauthorized decoding of encrypted message
  - Defined for each application
    - Examples:
      - Military orders = 1 hour to 3 years
      - Check transactions = 1 year
      - Business agreements = 10-15 years

Classical Cryptography

- Basic techniques for classical ciphers
  - ***Substitution:*** One letter is exchanged for another
  - ***Transposition:*** The order of the letters is rearranged
- Classical ciphers
  - ***Mono-alphabetic:*** Letters of the plaintext alphabet are mapped into ***other unique*** letters
  - ***Poly-alphabetic:*** Letters of the plaintext alphabet are mapped into letters of the ciphertext space depending on their ***positions*** in the text

Substitution

- Substitute each letter in the plaintext for another one.
- *Example* (Caesar Cipher)
  - 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
  - q e r y u i o p a s d f g w h j k l z x c v b n m t

Plaintext: under attack we need help

Ciphertext: cwyul qxxqrd bu wuuy pufj

Transposition

- Change the positions of the characters in the plaintext
- ***Example:***
  - Plaintext: meet me after the toga party
    - m e m a t r h t g p r y
    - e t e f e t e o a a t
  - Ciphertext: MEMATRHTGPRYETEFETEOAAT

Four Secure Key Distribution Strategies for Symmetric Cryptosystems

1. A key **K** can be selected by A to be shared with B, and **K** needs to be ***physically delivered*** to B
2. A third party can select the same key **K** and ***physically deliver*** **K** to A and B
3. If A and B have ***previously used*** a key **K'**, one party can ***transmit*** the new key **K** to the other, ***encrypted*** using the old key **K'**
4. If A and B each has an ***encrypted connection*** to a third party C, C can ***transmit*** the new key **K** on the ***encrypted links*** to both A and B

Asymmetric Key Cryptosystem
(Public Key Cryptosystem)

- Uses public and private keys
  - Public key for encryption
  - Private key for decryption
- Examples:
  - RSA
  - Trapdoor one-way function
  - Elliptical curve cryptography

Secure Communication

Two parties, Alice and Bob, can exchange information over an ***insecure medium*** in such a way that even if an intruder (Willie) is able to intercept, read and perform computation on the intercepted information, Willie will not be able to decipher the content of the exchanged information.

Encryption May Not Be Enough

- Prisoners Problem:
  - Alice and Bob are in jail and wish to hatch an escape plan. All their communications pass through the warden,Willie, and if Willie detects any encrypted messages, he can simply stop the communication.
- So they must find some way of hiding their secret message in an innocuous looking text.

Steganography

- In Greek, steganography means "***covered writing***"
- The art of ***hiding information*** is ways that ***prevent detection of hidden messages***.
- Steganography and cryptography are cousins in the spy craft family
- Different goals:
  - Cryptography: conceal the ***content*** of the messages
  - Steganography: conceal the ***existence*** of the messages

Steganography (cont.)

- What to hide
  - Texts
  - Images
  - Sound
  - ……
- How to hide
  - embed text in text/images/audio/video files
  - embed image in text/images/audio/video files
  - embed sound in text/images/audio/video files

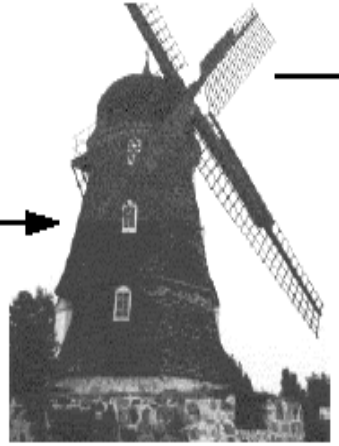
A Real Steganographic Example

- During WWI the following cipher message was actually sent by a German spy
  - "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils"
- Hidden Message
  - "Pershing sails from NY June 1"
  - How to extract the hidden message from the sent message?

A Steganographic System

carrier medium

embedding function



steganogram

extracting function

1010010101111
1010001100110
1111010111011
1001100100100
0100111100000
1011011011...

message to embed

1010010101111
1010001100110
1111010111011
1001100100100
0100111100000
1011011011...

extracted message

Digital Watermarking

- Used primarily for identification and embedding a unique piece of information within a medium without ***noticeably altering the medium***
- The difference between steganography and watermarking is primarily ***intent***.
  - ***Steganography conceals information;***
  - ***Watermarks extend information and become an attribute of the cover image***
- Publishing and broadcasting industries are interested in techniques for hiding ***encrypted copyright marks and serial numbers i***n digital films, audio recordings, books and multimedia products.

Applications of Digital Watermarking

- ***Copyright protection***
- ***Identification of financial instruments***, such as bills, coins, treasury bonds, cashier's checks, traveler's checks, notes, food stamps
- ***Fingerprinting*** (different recipients get differently watermarked content)
- ***Broadcast monitoring*** (television news often contains watermarked video from international agencies)
- Others

References

- M. E. Whitman and H. J. Mattord, *Principles of Information Security*, Thomson Course Technology, 5th edition, 2014.
- Stefan Katzenbeisser, Fabien A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Books, January 2000.
- Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, 2rd edition, November 2007.