Cryptography and Steganography

Professor Stephen S. Yau
Spring 2014

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
  - $K_\mathrm{d} \neq K_\mathrm{e}$

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:***
    - message: 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

Quantum Cryptography

- **Quantum cryptography** uses quantum mechanical effects (in particular quantum communication and quantum computation) to perform cryptographic tasks or to break cryptographic systems
  - Quantum communication (or qubit-communication)
    - Example: The parties can use exchange of photons through an optical fiber to transmit data
  - Quantum computation
    - In a general computational state model, there are two definite states (0 or 1), whereas quantum computation uses qubits (quantum bits) which can be a superposition [0 and/or 1] of both the states
  - Quantum mechanics
    - The body of scientific principles that explains the behavior of matter and its interactions with energy on the small scale of atoms and subatomic particles.

Quantum Cryptography (Cont.)

- Quantum cryptography uses (1) a quantum mechanical property of an electron existing partly in all its theoretically possible states simultaneously; but when measured or observed, gives a result corresponding to only one of the possible configurations, and (2) transmission of information in ***quantum states***, to implement a communication system that detects eavesdropping.
- **Quantum key distribution** (**QKD**)* describes the process to establish a shared key between two parties which include encoding the bits of the key as quantum states and transmitting them. If eavesdropper tries to learn these bits, the messages will be disturbed and can be easily detected due to the above quantum mechanical property

*http://en.wikipedia.org/wiki/Quantum_key_distribution

Quantum Cryptography *(Cont.)*

- Major advantages:
  - A key that is guaranteed to be secure can be produced, if the level of eavesdropping is below a certain threshold in the communication channel.
  - It allows the completion of various cryptographic tasks which are shown or conjectured to be impossible using only classical cryptographic techniques (example)
- Major limitation
  - Quantum cryptography can only provide 1:1 connection

Quantum Cryptography (Cont.)

- Protocols for Quantum Key Exchange,
  - BB84 protocol: Charles H. Bennett and Gilles Brassard
  - E91 protocol: Artur Ekert
- Some of the Quantum Key distribution networks,
  - DARPA
  - SECOQC
  - SwissQuantum
  - Tokyo QKD Network
  - Los Alamos National Labs
- The major advantage of quantum key distribution is its ability to detect any interception of the key

http://en.wikipedia.org/wiki/Quantum_cryptography

http://en.wikipedia.org/wiki/Quantum_key_distribution

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

Public Key Distribution and Authentication

- Using the “right” Public Key:
  - Must be **authentic**, not necessarily secret
- Obtaining the “right” Public Key:
  - *Directly* from its owner
  - *Indirectly*, in a signed message from a *Certification Authority* (CA):
    - A ***Certificate*** is a digitally signed message from a CA binding a public key to a name
    - Certificates can be passed around, or managed in directories
    - Protocols for certificate generation: e.g. X.509 (RFC 2459), SPKI/SDSI

Elliptic Curve Cryptography

- **Elliptic curve *cryptography* (ECC)** is an approach to ***public-key cryptography*** based on the algebraic functions of elliptic curves over finite fields.
- Private key is computed from the public key in elliptic cryptosystem using the ***elliptic curve discrete logarithm*** function
- Elliptic-curve-based protocols exploits the mathematical infeasibility of finding the ***discrete logarithm*** of a random elliptic curve with respect to a known base point.
- Major advantage: Key size can be very short

http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

Elliptic Curve Cryptography (Cont.)

- Discrete logarithm-based protocols have been adapted to elliptic curves,
  - Elliptic curve Diffie–Hellman (ECDH) key agreement scheme
  - Elliptic Curve Integrated Encryption Scheme (ECIES),
  - Elliptic Curve Digital Signature Algorithm (ECDSA)
  - ECMQV key agreement scheme based on the MQV key agreement scheme.
  - ECQV implicit certificate scheme.

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 ***<u>content</u>*** of the messages
  - Steganography: conceal the ***existence*** of the messages

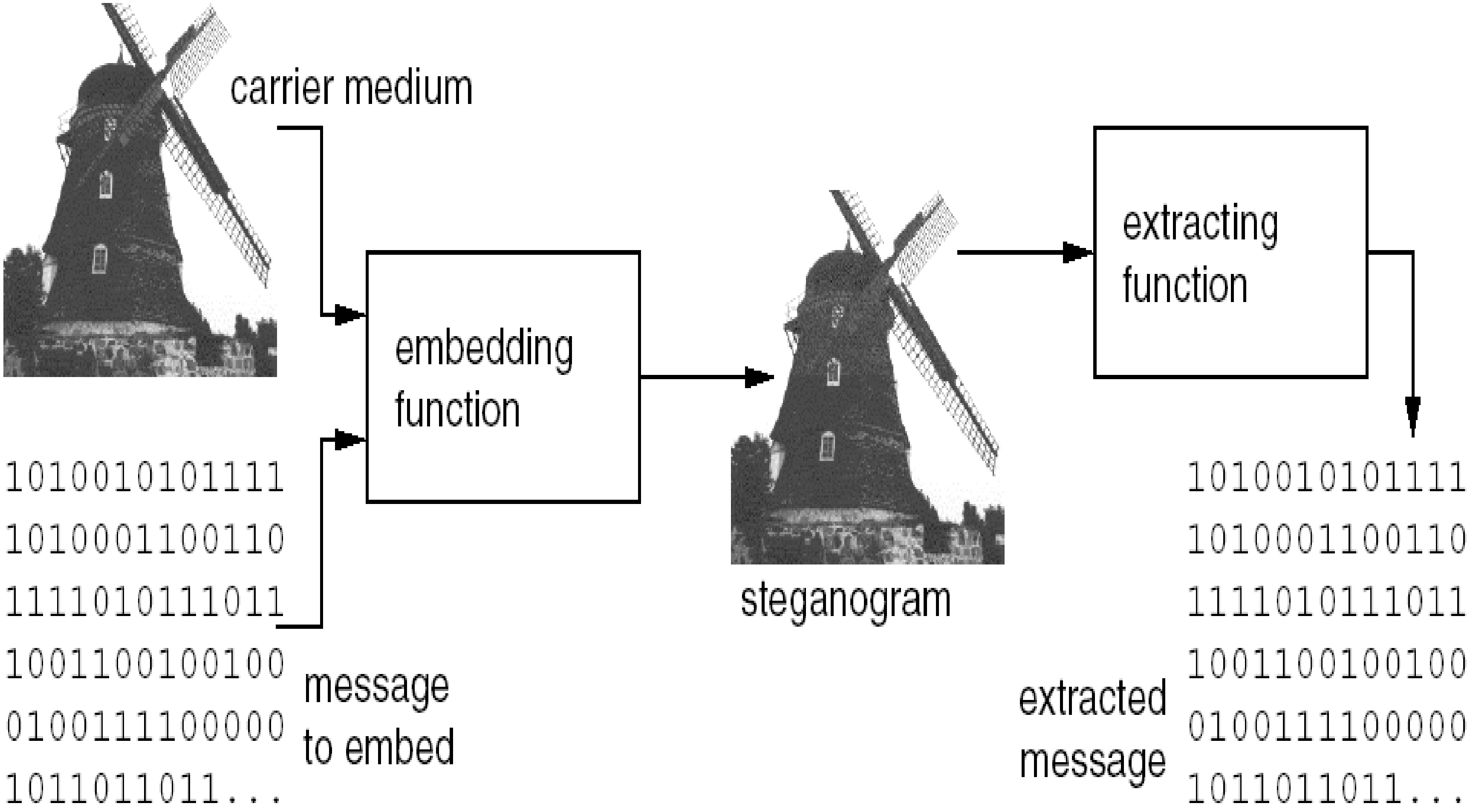
Steganography *(cont.)*

- 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

extracted message

1010010101111
1010001100110
1111010111011
1001100100100
0100111100000
1011011011...

References

- M. E. Whitman and H. J. Mattord, *Principles of Information Security*, Thomson Course Technology, 4th edition, 2011, Chapter 8.
- Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, 2rd edition, November 2007.
- Stefan Katzenbeisser, Fabien A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Books, January 2000.