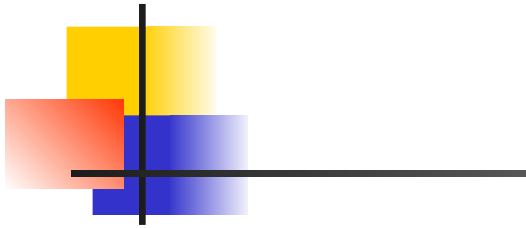
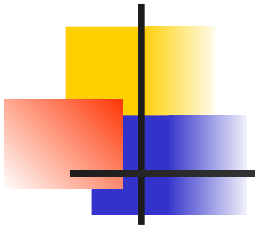


CSE 543
Information Assurance and Security

Cryptography

Professor Stephen S. Yau

Fall 2022

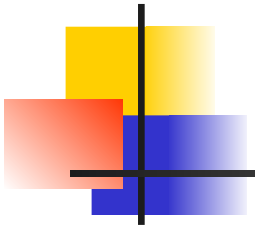


Cryptography

- In Greek means “secret writing”
- An interceptor, intruder or adversary can make following threats:
  - Block message
  - Intercept message
  - Modify message
  - Fabricate message

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



Cryptography (cont.)

- The basic component of cryptography is a ***cryptosystem***

- ***Cryptology: Study*** of ***encryption and decryption***, including cryptography and cryptanalysis.

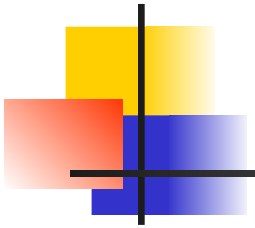
Cryptosystem

- *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 functions, D: $C \times K \rightarrow M$ is the set of deciphering functions.



Types of Cryptosystems

- ***Symmetric*** cryptosystems are ***classical cryptosystems***:

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

  - K, is the encryption/decryption key

Types of Cryptosystems (cont.)

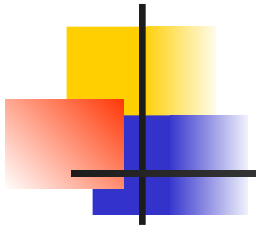
- ***Asymmetric*** cryptosystems:

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

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

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 to ***other unique*** letters
  - ***Poly-alphabetic:*** Letters of the plaintext alphabet are mapped to letters of the ciphertext space depending on their ***positions*** in the text

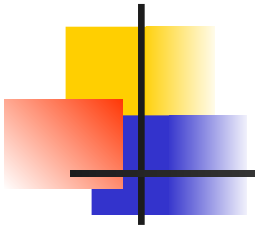


Substitution

- 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

Symmetric Cryptosystems
Four Secure Key Distribution Strategies

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

Symmetric Cryptosystems
Four Secure Key Distribution Strategies (cont.)

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 can be used for encryption (or decryption)
  - Private key can be used for decryption (or encryption)
- 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

Encryption in Android Devices

- Android has two methods for device encryption:
  - file-based encryption
  - full-disk encryption.

Encryption in Android Devices (cont.)

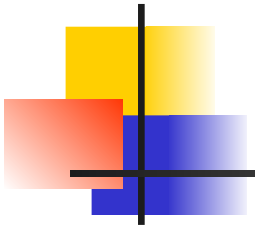
- ***File-based encryption:***
  - Android 7.0 and later supports file-based encryption. File-based encryption allows different files to be encrypted with different keys that can be unlocked independently. Devices that support file-based encryption can also support Direct Boot, which allows encrypted devices to boot straight to the lock screen, thus enabling quick access to important device features like accessibility services and alarms.

Encryption in Android devices (cont.)

- ***Full-disk encryption:***
  - Full-disk encryption is the process of encoding all user data on an Android device using an encrypted key. Once a device is encrypted, all user-created data is automatically encrypted before committing it to disk and all reads automatically decrypt data before returning it to the calling process.

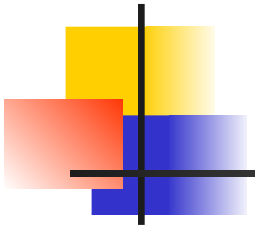
Homomorphic Encryption

- Perform computations on homomorphically encrypted data without decryption, and the result is in the form of plain text.
  - Obscurification?
  - Provide privacy-preserving storage. (why?)



Steganography

- In Greek, steganography means "***covered writing***"
- ***Prevent detection of hidden messages***
- Goals of cryptography and steganography:
  - 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 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?

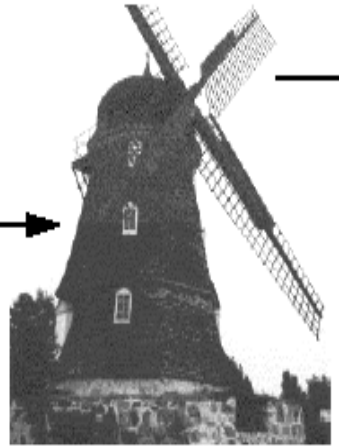
A Steganographic System

carrier medium

embedding function

1010010101111
1010001100110
1111010111011
1001100100100
0100111100000
1011011011...

message to embed

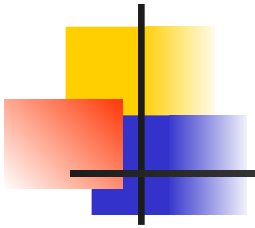


steganogram

extracting function

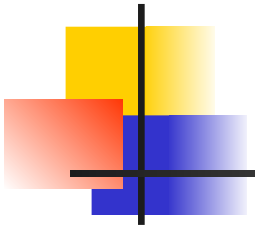
1010010101111
1010001100110
1111010111011
1001100100100
0100111100000
1011011011...

extracted message



Digital Watermarking

- Used primarily for identification and embedding a unique piece of information within a medium without noticeably altering the medium



Digital Watermarking

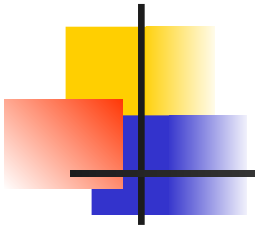
- ***Publishing and broadcasting industries*** are interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.

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

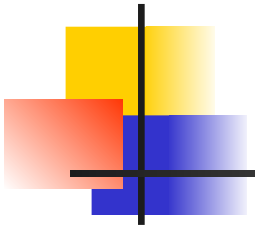
Applications of Digital Watermarking

- ***Broadcast monitoring*** (television news often contains watermarked video from international agencies)
- Others



Digital Signature

- A mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very high confidence that the message was created by a known sender (authenticity), and that the message was not altered in transit (integrity).



Digital Signature (cont.)

- Standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.
- Example - biased blind multisignature

Digital Signature (cont.)

- A digital signature scheme typically consists of three algorithms:
  - A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
  - A signing algorithm that, given a message and a private key, produces a signature.
  - A signature verifying algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Advantages of Digital Signature

- **Authentication**
  - Can be used to authenticate the identity of the source messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.
- **Non-repudiation**
  - An entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Advantages of Digital Signature (cont.)

- **Integrity**
  - If a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions

References

- M. E. Whitman and H. J. Mattord , Principles of Information Security, 7th edition, Thomson Course Technology, June 27, 2021. ISBN-10: 035750643X, ISBN-13 : 978-0357506431
- Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, 2nd edition, November 2007.
- A. B. Levina, V. Y. Kadykov and D. I. Kaplun, "New direction in Cryptography: Homomorphic Encryption," 2021 International Conference Automatics and Informatics (ICAI), 2021, pp. 234-237, doi: 10.1109/ICAI52893.2021.9639809.
- Encyprion and Data Protection, https://source.android.com/docs/security/encryption