Review of Quiz 1

**Info security**

Introduction:

* security objectives, security techniques, security trade-offs

Introduction to Cryptography, Secret Key and Public Key Cryptography

      Security objectives: ※ List and discuss recent trends in computer security ※ Describe simple steps to take to minimize the possibility of an attack on a system ※ Describe various types of threats that exist for computers and networks ※  Discuss recent computer crimes that have been committed

      Security techniques: \* Prevention \* Detection \* Recovery \* Tolerance \* Security by Obscurity \* Security by legislation

      substitution(simple alphabetic ~),permutation, combinations and iterations of ~ and ~

      Security trade-offs: confidentiality, integrity, availability VS cost, functionality, ease of use

      security problems: someone intercepts and reads(Confidentiality), intercepts and alters(Integrity),pretending to be Alice forges a message and sends to Bob(Authentication),Alice denies sending of the message(Non-repudiation of origin,Digital signature),denies the receipt of the message(Non-repudiation of the destination)

      Introduction to cryptography:

      Secret key:见下

      Public key: In public key encryption, two different keys are used to encrypt and decrypt the data. These two keys are mathematically related. One is the public key and other is the private key. They come as a pairs. (also known as a symmetric key encryption) public key is public to anyone. While the private key belongs only to the person who creates these two keys. The public key encryption to encrypt the sender’s message starts with the receiver, not the sender.  here is how it works:  First, Mary creates a pair of keys: one public key and one private key. She keeps the private key and gives the public key to Tom. After Tom writes his message, he uses the public key to encrypt it. When Mary gets the encrypted document, she uses the private key to decrypt it. The private key is only known to the receiver.

        here is another example.  Bob wants to send an encrypted message to Alice. They agree to use the public key encryption. Who creates keys? Who uses the public key? Who uses the private key? How many steps in the whole process?  Step 1: Alice creates a pair of keys: Public key and Private key. Alice puts the public key in a public key server which any one can access. Step 2: Alice informs Bob where he can get her public key. Step 3: Bob gets Alice’s public key. Step 4: Bob writes a message and uses Alice’s public key to encrypt it. Step 5: Bob sends his encrypted message to Alice. Step 6: Alice uses her own private key to decrypt Bob’s message.

      (Disadvantage) Although Alice’s private key can verify no one read or changes the document in transport, it cannot verify the sender. Because Alice’s public key is public, anyone can use it to encrypt his document and send it to Alice. While pretending to be Bob. In order to prove the sender, they need another technique: digital signature.

一些要知道的缩写：M = plaintext message, K = Key(Encryption Algorithm), C=E(K,M), M=D(K,C), C = Cipher-text message D  = Decryption Algorithm

* secret key crypto system, basics, how does it work, advantages and disadvantages, DES, Triple DES, AES, different modes (ECB,CBC, OFB,CFB, CTR)
  + (Secret Key, how does it work)A secret key crypto system uses only one key for both the encryption and decryption process. This one key is the secret key or the private key. Both the sender and receiver of the message has the private key. This is why it’s called symmetric key. The sender uses an algorithm and the key to encrypt the message the send it to the receiver, the receiver uses the same private key to decrypt the message.
  + (Secret Key, advantages) ◇ solves confidentiality and integrity ?s. ◇ can be used for Authentication ◇ can be used to securely store information on insecure media ◇ Integrity check
  + (Secret Key, disadvantages) ◇ doesn’t scale well (with N parties we need to generate and distribute N\*(N-1)/2 keys) ◇ key distribution problem: how to get the key to Alice and Bob? And to others? ◇ if everyone knows the key, it is no longer a secret.
  + Basics:
  + DES, Triple DES (Data Encryption Standard) 56bits—112bits ,is a product cipher with 56 bit key and 64 bit block size for plaintext and cipher-text (facts: □ efficient to implement in hardware, but relatively slow if implemented in software □ Encryption and Decryption algorithms are public, but the design principles are classified
  + AES (Advanced Encryption Standard) Asked interested parties worldwide to submit encryption algorithms for review  
    features：①unclassified, royalty-free algorithms②support 128-bit block sizes and 128-, 192-, and 256- bit key sizes
  + ECB, Electronic Codebook Book(what)♡message is broken into independent blocks that are encrypted ♡each block is a value which is substituted, like a codebook, hence name ♡ each block is encoded independently of the other blocks ♡ uses: secure transmission of single values (advantages and limitations) ღ message repetitions may show in cipher-text ღ weakness is due to the encrypted message blocks being independent ღ vulnerable to cut-and-paste attack ღ main use is sending a few blocks of data
  + CBC, Cipher Block Chaining（what）☞ main use is sending a few blocks of data  ☞ linked together in encryption operation ☞ each previous cipher block is chained with current plaintext block, hence name ☞ use Initial Vector (IV) to start process  ☞ IV prevents same P from making same C ☞ uses: bulk data encryption, authentication （advantages and limitations）☞ a cipher-text block depends on all blocks before it ☞ any change to a block affects all following cipher-text blocks ☞  need Initialization Vector
  + CFB, Cipher FeedBack （what）× message is treated as a stream of bits  × added to the output of the block cipher  × result is feed back for next stage (hence name)  × standard allows any number of bits (1,8, 64 or 128 etc) to be feed back ×  most efficient to use all bits in block (64 or 128)× uses: stream data encryption, authentication
  + CTR, Counter (what) ＊ a “new” mode, though proposed early on ＊ similar to OFB but encrypts counter value rather than any feedback value ＊ must have a different key & counter value for every plaintext block (never reused) ＊uses: high-speed network encryptions
* public key crypto system, basics, how does it work, advantages and disadvantages,

       RSA, Diffie Hellman, elliptic curve crypto

         ☆ RSA

         ☆ Diffie-Hellman,  elliptic curve crypto

* how current implementations eliminate the disadvantages of the public and secret key crypto system (digital envelope)
  + We use a digital signature to allow the receiver of the message to know who the message came from
  + A digital signature is equivalent to a handwritten signature, it is an electronic verification of the sender.   A digital signature serves 3 purposes:
    - 1) Authentication(who the message came from and its proof)
    - 2) Non-repudiation(now that receiver have record, the sender can’t deny the existence of the message)
    - 3) Integrity (the message was not corrupted, damaged, or changed during the transit)