8. Foundations of Cryptology

- Terminology
  - Algorithm
    - The mathematical formula or method used to convert an unencrypted message into an encrypted message.
  - Bit Stream Cipher
    - An encryption method that involves converting plaintext to ciphertext one bit at a time
  - Block Cipher
    - An encryption method that involves dividing the plaintext into blocks or sets of bits and then converting the plaintext to ciphertext one block at a time.
  - Cipher
    - The transformation of the individual components of an unencrypted message into encrypted components or vice versa.
    - The process of encryption or the algorithm used in encryption
  - Ciphertext or Cryptogram
    - The unintelligible encrypted or encoded message resulting from an encryption
  - Code
    - The process of converting components of an unencrypted message into encrypted components
  - Decipher
    - See Decryption
  - Decryption
    - The process of converting an encoded or enciphered message back to its original readable form
  - Encipher
    - See encryption
  - Encryption
    - The process of converting an original message into a form that cannot be used by unauthorized individuals.
  - Key or Cryptovariable
    - The information used in conjunction with the algorithm to create the ciphertext from the plaintext.
  - Keyspace
    - The entire range of values that can be used to construct an individual key
  - Link Encryption
    - A series of encryptions and decryptions between a number of systems, wherein each system in a network decrypts the message sent to it and then re-encrypts the message using different keys and sends it to the next neighbor
  - Plaintext or Cleartext
    - The original unencrypted message
  - Steganography
    - The process of hiding messages
  - Work Factor

- The amount of effort required to perform cryptanalysis on an encoded message

Cipher Methods

- ## Substitution Cipher
  - Exchanges one value for another
  - Monoalphabetic substitution:
    - Only incorporates a single alphabet in the encryption process
  - Polyalphabetic Substitution:
    - Incorporates two or more alphabets in the encryption process.
  - Vigenere cipher
    - Polyalphabetic code of 26 distinct cipher alphabets
    - Uses a Vigenere square
      - 26x26 table
- ## Transposition Cipher
  - Rearranges the bits or bytes within a block based on an established pattern to create the ciphertext.
- ## Exclusive OR (XOR)
  - A function of boolean algebra where two bits are compared and a binary result is generated
  - If the two bits are identical, return 0
  - If two bits are not identical, return 1
- ## Vernam Cipher
  - Developed by AT&T known as the ‘one-time pad’
  - Uses a set of characters for encryption ops only one time and then discards it.
- ## Book-Based Ciphers
  - Ciphertext consists of a list of codes representing the page number, line number, and word number of the plaintext words.
- ## Hash Functions
  - Mathematical algorithms used to confirm the identity of a specific message and confirm that the content has not been changed.
  - They do not create ciphertext, they confirm message identity and integrity.
  - Hash value
    - Created by converting variable-length message into a single fixed-length value.
    - Message digest is a fingerprint of the author's message that is compared with the recipients locally calculated hash of the same message.
    - They do not require the use of keys but is possible to attach a message authentication code (MAC).
    - Salting
      - Providing a random set of values to the hashing algorithm to produce a second hash

        - Takes away an attackers incentive and time-memory-tradeoff is no longer in the attackers favor.
    - Used in password verification systems to store passwords and confirm the identity of the users

Cryptographic Algorithms

- Symmetric Encryption (Private Key Encryption)

- Encryption methodologies that require the same key
    - The same algorithm and ‘secret’ are used both to encipher and decipher the message
    - Both sender and receiver must possess the same secret key
    - If either key is compromised, messages can be decrypted and read without sender/receiver knowledge
- Encryption and decryption happen fast
- Popular Symmetric Cryptosystems
    - **Data Encryption Standard (DES)**
        - 128 key length
        - 64 bit block size
        - 56 bit key
    - **3DES**
        - Created to provide a level of security far beyond that of DES
    - **Advanced Encryption Standard (AES)**
        - Rijndael Block cipher with a variable key length of 128, 192, or 256 bits
        - Built to replace DES and 3DES

- Asymmetric Encryption (Private Key, Public Key)

- Uses two different but related keys (Public Key, Private Key)
    - Either key can be used to encrypt or decrypt a message.
    - If key A encrypts a message, only key B can decrypt it. Vice versa
- Best if one key used as a private key and the other as a public key
- Simple to compute in one direction but difficult to compute in the opposite direction
- **RSA**
    - First published for public use in 1977
    - The defacto standard for public-use encryption applications.
    - Holding a single conversation between two parties requires 4 keys,

- Encryption Key Size
    - The larger the key the longer it takes to guess.

Cryptographic Tools

- Public Key Infrastructure (PKI)

- PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities.
    - Digital certificates allow the PKI components and their users to validate keys and identify key owners.
- PKI systems and their digital certificate registries enable the protection of information by making verifiable digital certificates readily available to business applications. This allows businesses to implement characteristics of infosec into their organizations
    - Authentication
    - Integrity
    - Privacy
    - Authorization
    - Nonrepudiation
- Components
    - Certificate Authority (CA)
        - Issues, manages, authenticates, sign, and revokes users' digital certificates.
    - Registration Authority (RA)
        - Handles certification functions such as verifying registration information, generating end-user keys, revoking certificates, and validating user certificates, in collaboration with the CA
    - Certificate directories
        - Central locations for certificate storage that provide a single access point for administration and distribution
    - Management protocols
        - Organize and manage communications around CAs, RAs, and end-users.
        - Includes the functions and procedures for setting up new users, issuing keys, recovering keys, updating keys, revoking keys and enabling the transfer of certificates and status information
    - Policies and procedures
        - Assign an organization in the application and management of certificates, in the formalization of legal liabilities, and in actual business use.

- Digital Signatures

- Created to verify information transferred via electronic systems.
- Encrypted messages that can be mathematically proven as authentic.
- Private key used to encrypt a message, public key used to decrypt the message.
- Should be created using Digital Signature Standard (DSS)
- Help authenticate the origin of a message.
- Created with asymmetric encryption processes

- ### Digital Certificates
    - An electronic document or container file that contains a key value and identifying information about the entity that controls the key.
    - Certificate often issued and certified by a third party (Certificate Authority)
    - Digital certificates authenticate the cryptographic key that is embedded in the certificate
- ### Hybrid Cryptography Systems
    - Pure asymmetric key encryption is not widely used (With the exception of **digital certificates**)
    - Diffie-Hellman key exchange
        - Most common hybrid system
        - Uses asymmetric encryption to exchange session keys
            - Session keys are limited-use symmetric keys that allow two entities to conduct quick, efficient, secure communications based on symmetric encryption, which is more efficient than asymmetric encryption for sending messages.
        - Provides the foundation for subsequent developments in public-key encryption.
        - Protects exposure to third parties
- ### Steganography
    - *The art of secret writing*
    - Hiding things in plain sight, like an image.

Protocols for Secure Communications

- ### Internet Communications S-HTTP and SSL
    - **SSL**
        - Invented by Netscape to use public-key encryption to secure a channel over the internet.
        - Heartbeat bug found in 2004 allowed to bypass some controls.
        - SSL Record Protocol
            - Responsible for the fragmentation, compression, encryption, and attachment of an SSL header to the plaintext prior to transmission.
            - Received encrypted messages are decrypted and reassembled for presentation to the higher levels of the protocol. L
    - **Secure - HTTP. (S-HTTP)**
        - Provides the Internet communication services between client and host without consideration for encryption of the data that is transmitted between client and server.
        - Extended version of HTTP that provides for the encryption of individual messages transmitted via the internet between a client and server.
        - S-HTTP is the application of SSl over HTTP
            - Must have a session open
            - S-HTTP client sends the server its public key so that the server can generate a session key.
            - Session key is encrypted and returned to the client.

        - S-HTTP can provide confidentiality, authentication and data integrity through a variety of trust models and cryptographic algorithms.
- Email with S/MIME, PEM and PGP
    - **Secure Multipurpose Internet Mail Extensions (S/MIME)**
        - Builds on the encoding format of the MIME protocol and uses digital signatures based on public-key cryptosystems to secure email.
            - SMTP had limitations and was replaced with MIME
        - Has the option to sign, encrypt and decrypt messages.
    - **Privacy-Enhanced Mail (PEM)**
        - Proposed standard to use 3DES symmetric key encryption and RSA for key exchanges and digital signatures.
            - Never widely deployed.
    - **Pretty Good Privacy (PGP)**
        - Developed by Phil Zimmerman and uses the IDEA cipher for message encoding
        - Also uses RSA for symmetric key exchange and digital signatures.
- Web Transactions
    - **SET**
        - Secure Electronic Transactions
        - Developed by mastercard and visa in 1997 to protect against electronic payment fraud.
        - SET uses DES to encrypt credit card information transfers and RSA for key exchange.
        - Provides protection for internet and retail swype based transactions
    - **SSL**
        - Mainly relies on RSA for key transfer and uses IDEA, DES, or 3DES for encrypted symmetric key-based data transfer.
    - S-HTTP
    - SSH-2
    - IPSec
- Wireless Networks with WEP and WPA
    - **Wired Equivalent Privacy (WEP)**
        - Early attempt to provide security with the 802.11 protocol.
        - Cryptographically weak.
            - Key management is not effective because most networks us a single shared secret key value for each node.
                - Synchronizing key changes is a tedious process and no key management is defined in the protocol.
            - The initialization vector (IV) is too small, resulting in the recycling of IVs.
                - An attacker can reverse engineer the RC4 cipher stream and decrypt subsequent packets, or can forge future packets.
        - Uses RC4 cypher stream to encrypt each packet using a 64-bit key.
            - Key is created using a 24-bit initialization vector and a 40bit key value.
            - Packets are formed with an XOR function to use the RC4 key value stream to encrypt the data packet.
            - 4-byte integrity check value (ICV) is calculated for each packet and then appended.
    - **WPA & WPA2**

- WPA
    - was a temp replacement for WEP.
    - WPA uses 128 bit key size instead of static keys.
    - Uses dynamic keys created and shared by an authentication server
        - Via Temporal Key Integrity Protocol (TKIP)
            - TKIP algorithms are backwards compatible with legacy devices.
            - A cryptographic message integrity code, or MIC, to defeat forgeries.
            - A new IV sequencing discipline to remove replay attacks from the attackers arsenal
            - A per-packet key mixing function to decorrelate the public IVs from weak keys
            - A rekeying mechanism to provide the fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse.
- WPA2
    - Replaces WPA.
    - Uses AES-based encryption.
    - Backwards compatible with WPA

- **Next Gen Wireless Protocols**
    - Robust Secure Network (RSN)
        - A protocol for establishing secure communications over an 802.11 wireless network. (802.11i)
        - RSN uses AES along with 802.1x and EAP.
        - RSN extends AES with CCMP.
        - AES supports key lengths of up to 256 bits.
        - RSN protocol functions:
            - The wireless NIC sends a probe request
            - Wireless access point sends a probe response with an RSN Information Exchange (IE) frame
            - Wireless NIC requests authentication via one of the approved methods
            - The wireless access point provides authentication for the wireless NIC
            - The wireless NIC sends an association request with an RSN IE frame
            - The wireless access point sends an association response.
    - Bluetooth
        - 30ft range
        - Discoverable mode makes your vulnerable
        - So does other devices previously attached.
        - Don't have BT on when not in use.

- TCP/IP with IPSec and PGP

- **IPSec**
    - An open-source protocol framework for security development within the TCP/IP family of protocol standards.
    - Used to secure communications across IP-based networks such as LANs, WANs and the Internet.
    - Often used to create VPNs

- Uses several different cryptosystems
    - Diffie-Hellman key exchange for deriving key material between peers on a public network
    - Public-key cryptography for signing the Diffie-Hellman exchanges to guarantee identity.
    - Bulk encryption algorithms for encrypting the data.
    - Digital certificates signed by a certificate authority to act as digital ID cards.
- Operates in two modes
    - Tunnel Mode
        - The entire packet is encrypted and placed in the content portion of another IP packet.
    - Transport Mode
        - Only IP data is encrypted, not the headers.
- Application Header (AH) protocol
    - Provides system-to-system authentication and data integrity verification but does not provide secrecy for the content of a network communication
    - Designed to provide data integrity and IP packet authentication.
        - Protected against replay attacks and address spoofing.
- Encapsulating Security Payload (ESP) protocol
    - Provides secrecy for the contents of network communications as well as system-to-system authentication and data integrity verification

- **PGP**
    - Designed in 1991 by Phil Zimmermann
    - 6-services
        - Authentication by digital signatures
        - Message encryption
        - Compression
        - E-mail compatibility
        - Segmentation
        - Key management.
    - Uses freeware zip algorithm to compress message after it has been digitally signed but before it is encrypted.
        - Smaller file, less data to give to hackers.
    - Can provide segmentation of messages.
    - Trust can be assigned and addressed and assured by using the public key-ring.

Function	Algorithm	Application
Public-key encryption	RSA/SHA-1 or DSS/SHA-1	Digital signatures

Conventional encryption	3DES, RSA, IDEA, or CAST	Message encryption
File management	ZIP	Compression

Chapter Summary

- Encryption is the process of converting a message into a form that is unreadable to unauthorized people.
- The science of encryption, known as cryptology, encompasses cryptography (making and using encryption codes) and cryptanalysis (breaking encryption codes).
- Cryptology has a long history and continues to change and improve.
- Two basic processing methods are used to convert plaintext data into encrypted data—bit stream and block ciphering. The other major methods used for scrambling data include substitution ciphers, transposition ciphers, the XOR function, the Vigenère cipher, and the Vernam cipher.
- The strength of many encryption applications and cryptosystems is determined by key size. All other things being equal, the length of the key directly affects the strength of the encryption.
- Hash functions are mathematical algorithms that generate a message summary, or digest, that can be used to confirm the identity of a specific message and confirm that the message has not been altered.
- Most cryptographic algorithms can be grouped into two broad categories: symmetric and asymmetric. In practice, most popular cryptosystems are hybrids that combine symmetric and asymmetric algorithms.
- Public key infrastructure (PKI) is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely. PKI includes digital certificates and certificate authorities.
- Digital signatures are encrypted messages that are independently verified by a central facility, and which provide nonrepudiation. A digital certificate is an electronic document, similar to a digital signature, which is attached to a file to certify it came from the organization that claims to have sent it and was not modified from its original format.

- Steganography is the hiding of information. It is not properly a form of cryptography, but is similar in that it is used to protect confidential information while in transit.
- S-HTTP (Secure Hypertext Transfer Protocol), Secure Electronic Transactions (SET), and SSL (Secure Sockets Layer) are protocols designed to enable secure communications across the Internet. IPSec is the protocol used to secure communications across any IP-based network, such as LANs, WANs, and the Internet. Secure Multipurpose Internet Mail Extensions (S/MIME), Privacy Enhanced Mail (PEM), and Pretty Good Privacy (PGP) are protocols that are used to secure electronic mail. PGP is a hybrid cryptosystem that combines some of the best available cryptographic algorithms; it has become the open-source de facto standard for encryption and authentication of email and file storage applications.
- Wireless networks require their own cryptographic protection. Originally protected with WEP and WPA, most modern Wi-Fi networks are now protected with WPA2. Bluetooth—a short-range wireless protocol used predominantly for wireless phones and PDAs—can be exploited by anyone within its 30-foot range.
- Most well-known encryption methods are released to the information security and computer security communities for testing, which leads to the development of more secure algorithms.

Review Questions

1. What are cryptography and cryptanalysis?
    a. Cryptography is the process of making and using encryption codes to secure messages whereas Cryptoanalysis is taking ciphertext and getting the plaintext message without the encryption keys
2. What was the earliest reason for the use of cryptography?
    a. Concealing military/political secrets.
3. What is a cryptographic key, and what is it used for? What is a more formal name for a cryptographic key?
    a. A string of data or information that determines the functional output of a cryptographic algorithm. Keys(or cryptovariables) are used to specify the transformation of a plaintext message into ciphertext.
4. What are the three basic operations in cryptography?
    a. Encrypting, Decrypting, Hashing
5. What is a hash function, and what can it be used for?
    a. A Hash Function is an algorithm that takes an input and returns a fixed-size string of bytes. A hash function is used to confirm the identity of a message and confirm that it hasn't been changed and is often used in password storage systems to confirm and verify identity.
6. What does it mean to be “out of band”? Why is it important to exchange keys out of band in symmetric encryption?
    a. ‘Out of Band’ refers to communications that do not carry the ciphertext
    b. Sending the key out of band is to prevent the key from being intercepted and used to read the message.
7. What is the fundamental difference between symmetric and asymmetric encryption?
    a. Symmetric encryption uses a Private Key while Asymmetric encryption uses a Public Key and a Private Key
8. How does public key infrastructure add value to an organization seeking to use cryptography to protect information assets?
9. What are the components of PKI?

    a. Certificate Authority
    b. Registration Authority
    c. Certificate Directories
    d. Management Protocols
    e. Policies and Procedures
10. What is the difference between a digital signature and a digital certificate?
    a. Digital signature verifies information transferred from electronic systems, while a digital certificate is a document that contains the key values for and identifying information about the entity that controls the key
11. What critical issue in symmetric and asymmetric encryption is resolved by using a hybrid method like Diffie-Hellman?
    a. Diffie-Hellman protects you from 3rd party risk and allows you to send keys without the need for the communication to be 'out-of-band'
12. What is steganography, and what can it be used for?
    a. The process of hiding messages in images/music/movies.
13. Which security protocols are predominantly used in Web-based e-commerce?
    a. SET, SSL, S-HTTP, SHA-2, IPSec
14. Which security protocols are used to protect e-mail?
    a. S/MIME, PGP, PEM
15. IPSec can be implemented using two modes of operation. What are they?
    a. Tunnel and Transport modes.
16. Which kind of attack on cryptosystems involves using a collection of pre-identified terms? Which kind of attack involves sequential guessing of all possible key combinations?
    a. A Dictionary Attack uses a file of pre-identified terms
    b. The type of attack where a script tries all combinations possible to crack your password. is called a Brute-Force attack,
17. If you were setting up an encryption-based network, what key size would you choose and why?

a. You would use the largest key that your protocol and time/budget allows.

18. What is the typical key size of a strong encryption system used on the Web today?
    a. SSL uses a 128-bit key
19. What encryption standard is currently recommended by NIST?
    a. AES (Advanced Encryption Standard)
20. What are the most popular encryption systems used over the Web?
    a. SSL, 3DES, AES, PGP, RSA