Cryptographic Technologies and Algorithms

Cryptography Basics

Ed Crowley

Fall '08

Topics: Symmetric & Asymmetric Technologies

- Kerckhoff's Principle
- Symmetric Crypto Overview
  - Key management problem
  - Attributes
  - Modes
  - Symmetric Key Algorithms
- DES
  - Attributes
  - Modes
  - 3DES
- AES
- Other Symmetric Ciphers
- Escrowed Encryption
- Symmetric Key Limitations
- Asymmetric Cryptography
  - Asymmetric Algorithms
  - Key Size Comparison
  - Hybrid Cryptosystems
  - RSA
  - Diffie-Hellman
  - El Gamal
  - Elliptic Curve
- Message Digests and Related One Way Functions

Scope

- Here, focus is on cryptographic technologies and algorithms that provide enterprise security services.
- Specific technologies include:
  - Secret key crypto
    - Related algorithms
  - Asymmetric key crypto
    - Related algorithms
  - Message Digests and Related One way functions

Symmetric/Asymmetric Key Technologies

- Symmetric key
  - Uses a single shared secret key.
    - aka secret key, private key, single key, or classic cryptography.
- Asymmetric key
  - Uses a pair of related keys
  - One key is public and one key is private (secret)
    - aka public key or two key cryptography.
    - Typically, public key is used to encrypt with private key used to decrypt

Message Digests

- A message digest is used as a proxy for a message, it is a shorter, redundant representation of that message. [1]
  - May also be called a hash, digital fingerprint, or a digest.

Two major types

1. MIC bound just to original document
2. MAC is bound to original document and sender (by a shared secret key)

- 1. H.X. Mel

Kerckhoff's Principle

For all civilian crypto systems, Kerckhoff's Principle is the law.

- All secrecy needs to be in the key.
  - 1883, Kerchhoff
- That is, the algorithm needs to be public.

- If the key is compromised there is no secrecy.
- If the key is lost, any encrypted documents are, likely, unrecoverable.

Symmetric Key Overview

- Classic cryptography
- Same shared key encrypts and decrypts
- Fast
  - Ideal for bulk encryption
  - 1000 to 10,000 times faster than public key cryptography.
- Problematic Key Management
  - Can only be used by prearrangement.
  - Key management issues preclude scaling
- Hybrid systems employ temporary session keys.

Asymmetric Key Overview

- Relatively, new (mid-'70's) cryptographic technology
- Utilizes two different, but mathematically related, keys.
  - Normally, public key is widely distributed
  - Only one person possesses private key (tied to identity)
- A message encrypted with one key can only be decrypted with the other.
  - Solves classic cryptography key management problem
  - In most cases, utilizes a relatively large key
  - Relatively slow
  - Depending on how employed, may provide confidentiality, integrity, authentication, or non-repudiation though, not all at the same time

Symmetric/Asymmetric Key Size Comparisons

- 80-bit private key roughly equivalent to a 1024-bit public key.
- 128-bit private key roughly equivalent to a 3000-bit public key.

Symmetric Key Encryption

- Normally, provides confidentiality.
  - For integrity and authentication, can be incorporated in a HMAC
- Single key, shared by sender and receiver.
  - aka conventional cryptography or single key cryptography.
  - aka Private Key Cryptography
- Key management problematic

Symmetric Key Management Problems

- Only works by prearrangement.
  - Cipthertext recipient must already posses key.
- Key distribution/management issues include:
  - How do you deliver the key to the recipient without someone intercepting it?
  - If two people have the key and it is compromised, whom is responsible?
  - If key is lost, cipher text cannot be decrypted.
- Does not scale well.
  - A system with N users requires N(N-1)/2, keys

Symmetric Key Management

Key management functions

- Generation
- Recording
- Transcription
- Distribution
- Installation
- Storage
- Change
- Disposition
- Control
- Other

Principles of key management

- No key may ever appear in the clear
- Keys must be chosen evenly from the entire key space
- Therefore keys should be randomly generated by a secure engine
- Key-encrypting keys must be separate from those keys used for other objects
- Everything encrypted under a key encrypting key must originate within a crypto engine
- Key management must be fully automated and independent of the user

Symmetric Key Attributes

- Fast, 1000 to 10,000 times faster than asymmetric crypto
  - Useful for encrypting large volumes of static data
- All security in the key
  - With large key sizes, can be very strong.
    - In this context, strong crypto refers to key sizes 128 or more bits
  - If key is compromised, then there is no confidentiality.

Symmetric Key Algorithms: DES

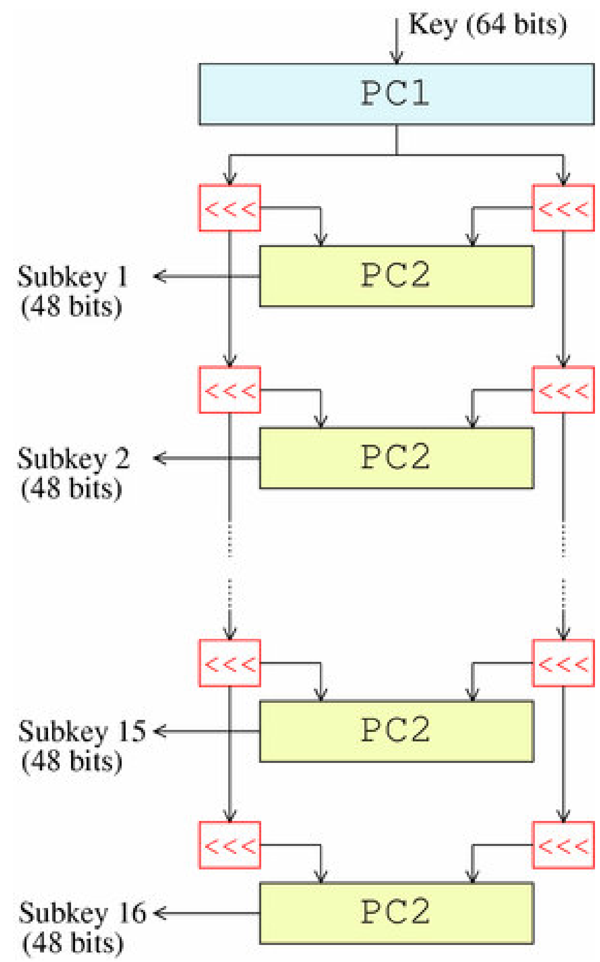
- First modern, secure symmetric encryption algorithm.
- Significant attributes:
  - Known in great detail
  - Free from patent issues
  - Generally accepted
- Relatively simple, uses only three functions
  - XOR
  - Permutation
  - Substitution
- Originally, designed for hardware implementation

Data Encryption Standard (DES)

- Symmetric key cryptosystem
  - DES describes the Data Encryption Algorithm (DEA).
  - Derived from IBM's Lucifer algorithm (1972)
  - Originally designed for hardware implementation.
    - Software implementations are considered slower than hardware implementations.
- 1975, proposed as national standard for "unclassified computer data".
  - Used for commercial and non-classified purposes.

DES/DEA Cryptosystem

- 16-round cryptosystem
  - Each round uses a unique 48 bit subkey
- 56 bit key (Shorter than Lucifer!!!)
  - 64 bits with 8 as a parity check
- 64 bit blocks.



Symmetric Key Modes: Block or Stream

Block

- Message divided into plain text blocks.
  - In turn, each block processed by an algorithm.
- Requires relatively less processing power.
  - More suitable to software implementation.

Stream

- Message treated as a stream of bits.
  - Each bit processed by an algorithm.
  - For example, in a one time pad, the message stream is XORed with the key.
- Requires relatively more processing power,
  - More suitable to hardware implementation.

Modes of Operation

- With a block cipher encrypt operation, whenever the same key is used, the same plaintext block will always encrypt to the same ciphertext block.
  - Certain kinds of data patterns in the plaintext, such as repeated blocks, are apparent in the ciphertext.
- Cryptographic modes of operation alleviate this problem by combining the basic cryptographic algorithm with variable initialization vectors and some sort of feedback.
  - NIST Recommendation for Block Cipher Modes of Operation [SP800-38] defines modes of operation for the encryption and decryption of data using block cipher algorithms
- Modes may require initialization vectors

Initialization Vector (IV)

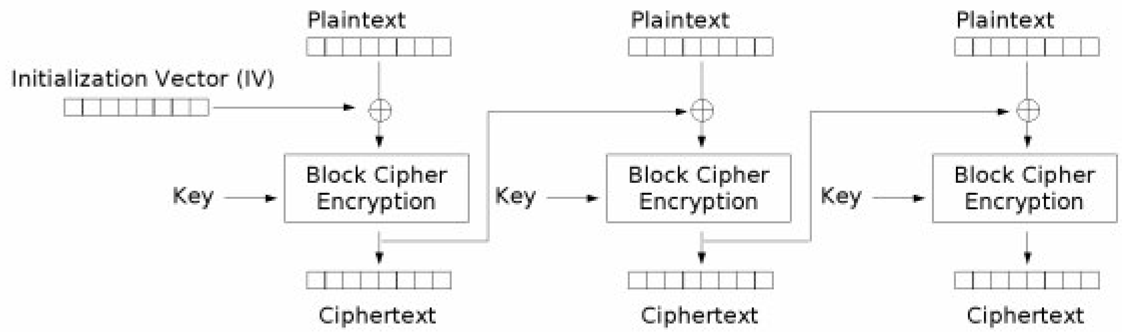
- Block of bits that that allows a stream or a block cipher to be executed in any of several streaming modes of operation to produce a unique stream independent from other streams produced by the same encryption key.
  - Depends on encryption algorithm and on cryptographic protocol in use.
    - Normally as large as cipher block or as large as key.
  - Must be known to the encrypted information's recipient
- WEP, the Wired Equivalent Privacy, (802.11 encryption algorithm) used a "weak IV" that led to it being easily cracked.

DES Modes

Four DES modes:

1. Cipher Block Chaining (Block)
2. Electronic Code Book (Block)
3. Cipher Feedback Mode (Stream like)
4. Output Feedback. (Stream like)

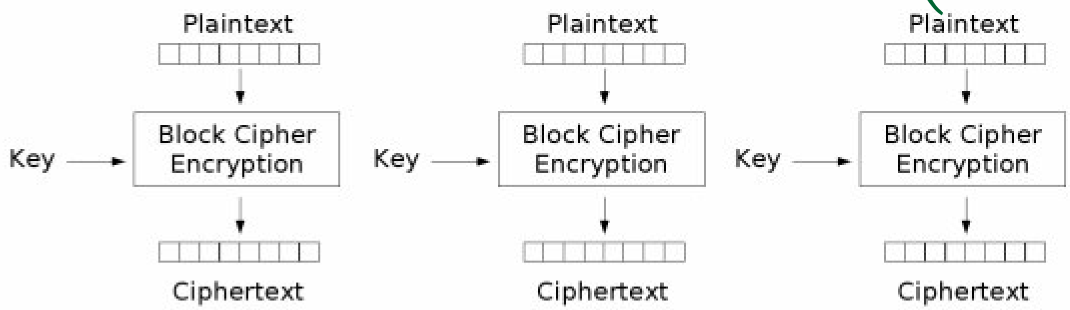
Cipher Block Chaining



Cipher Block Chaining (CBC) mode encryption

- Operates with 64 bit plaintext blocks.
- For each block, key value influenced by previous block .
- Consequently, identical patterns in different messages are encrypted differently.

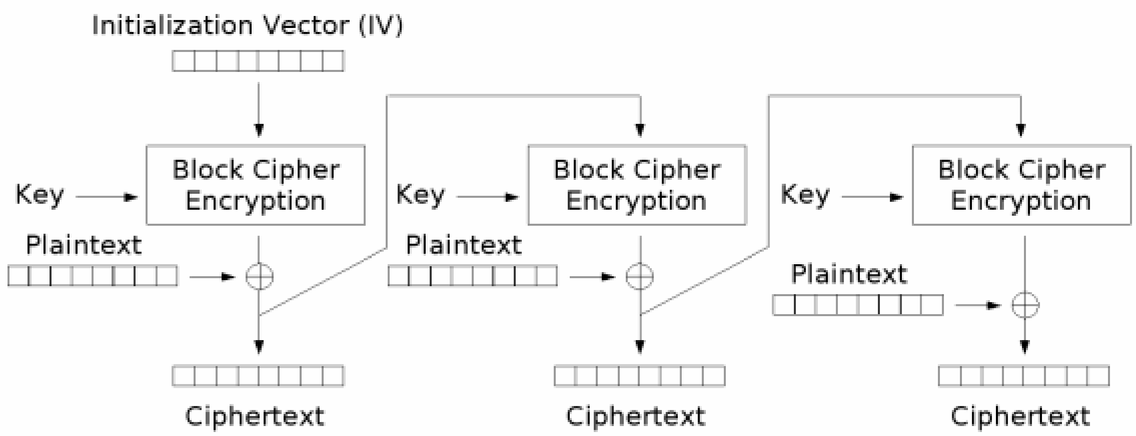
Electronic Code Book (ECB)



Electronic Codebook (ECB) mode encryption

- Each block encrypted independently.
  - Each cipher block corresponds to a plaintext block.
  - When the same pattern occurs, it is always encrypted the same.
- Native DES mode
  - Best suited for use with small amounts of data such as in a Data Base, ATM card, etc...

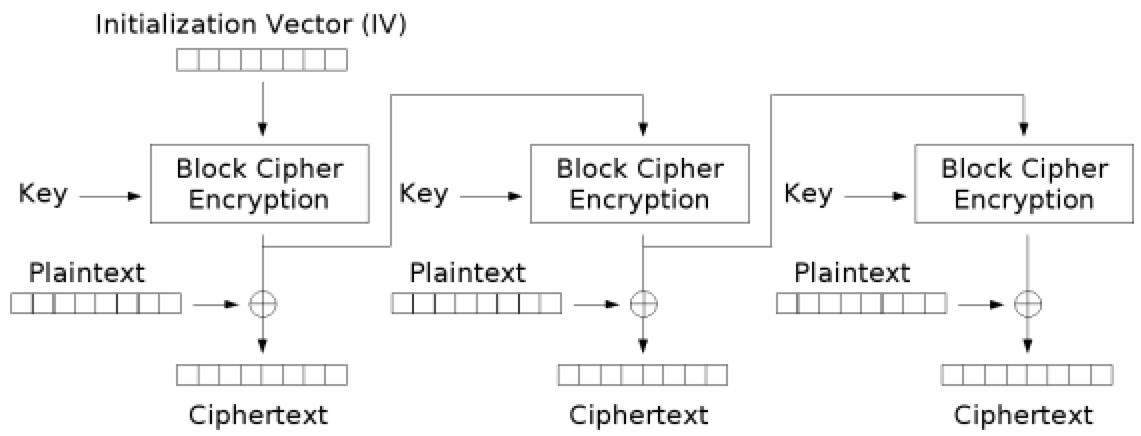
Cipher Feedback Mode (CFB)



Cipher Feedback (CFB) mode encryption

- CFB
  - Close relative of CBC.
  - Makes a block cipher into a self-synchronizing stream cipher.

Output Feedback



Output Feedback (OFB) mode encryption

- Output Feedback
  - DES generated stream cipher that is XORed with a message stream.
  - Simulates a one time pad.

DES Weaknesses

- Relatively short, 56 bit, fixed key length
- Fixed 64 bit block length
- Designed for Hardware implementation
  - Optimized for ’70s hardware
- Except for brute force, DES has proven resilient to all attacks
- Since November 1998, not US government approved.
  - Triple DES (3DES), replaced DES.
  - AES replaced Triple DES.

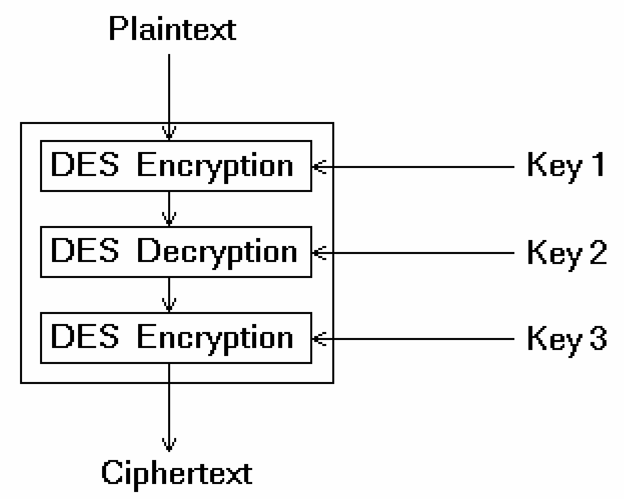
Brute Force Attacks: DES

- DES is vulnerable to brute force attacks.
  - 1997, a distributed brute force attack (14,000 machines, 4 months) succeeded
  - 1998, EFF demonstrated DES key cracking in 56 hours with a single $250,000 machine
  - 1999, EFF demonstrated a distributed attack that brute forced DES in 22 hours
  - http://cryptome.org/cracking-des.htm
- Moore's Law dictates that each year brute force attacks become more practical.

3DES

- Triple-DES originally recommended to replace DES.
  - 3DES has an effective 168 bit key length
    - 3X56
- As FIPS Standard, DES was replaced by AES (Advanced Encryption Standard)

3DES



- Utilizes three separate encryption actions
  - Not absolutely necessary to use 3 keys.
  - In practice, most applications use 2 keys.
- Eliminates most critical DES weakness – that of a short key length.
- Weakness is speed.

Advanced Encryption Standard (AES)

- Block cipher DES replacement.
- National Institute of Standards and Technology (NIST) initiative.
  - Announced January 1997.
- AES, aka Rijndael Block Cipher
  - New Federal Information Processing Standard (FIPS) replacing DES/3-DES.
  - US Government standard for protection of sensitive but unclassified information.

Rijndael Block Cipher

- Iterated block cipher
  - Variable block and key lengths
  - Can be independently chosen as 128, 192, or 256 bits.
- In contrast to a DES like Feistel network, that takes a portion of the modified plaintext and transposes it to another position, the Rijndael Cipher employs a round transformation that is compromised of three layers of distinct and invertible transformations.
- Compared to other algorithms, algorithm design is relatively simplistic. (Simple is good.)

Other Symmetric Ciphers

- Two Fish
  - Bruce Schneier led development for entry into NIST's post DES competition.
- IDEA
  - International Data Encryption Algorithm. Used in PGP (patented). 64 bit block cipher. 128 character key length
- RC4
  - Utilizes variable key size. Used in SSL. Inappropriately implemented in 802.11 WEP standard.
- RC5
  - Fast symmetric block cipher. Variable word size. Variable number of rounds. Variable-length secret key.

Escrowed Encryption

- Concept that divides key into two, or more, parts and stores the separate key portions with separate “trusted” organizations.
- When dealing with encryption keys, the same precautions must be used as with physical keys.

Clipper Chip/Key Escrow

- Historical governmental program that embeds Clipper chips into electronic devices
  - Based on an 80-bit implementation of classified Skipjack algorithm
- For easy access by law enforcement, government would hold key copies in escrow
  - Two key halves held by two different government agencies
- Eventually died due to a lack of public support

Three Symmetric Key Limitations

1. Key distribution problem
   1. Prior to communications, keys must be distributed out of band
2. Lacks scalability
   1. Number of keys increases with the square of number of users
3. Security services primarily limited to confidentiality

These limitations led to the development of Asymmetric Key Cryptography.

Note

- Most modern cryptosystems are hybrid systems.
  - That is, they use both symmetric and asymmetric methods.
- For example, in SSL the servers public key, from it's certificate, encrypts a temporary symmetric session key.

Asymmetric Cryptography

- Employs mathematically related key pairs
  - One key is public, one key is private
  - Unlike a shared symmetric key, an asymmetric private key is never shared.
  - Within a given key pair, keys are different but related
- Keys based upon problems that are easy to solve one way and very difficult to solve the other
  - For example, RSA utilizes, in part, the problem of factoring the product of two large primes
    - Easy to multiply, very, very difficult to factor
  - Other examples of difficult problems include those based upon discrete logarithms and elliptic curves
- Avoids Symmetrical Cryptography limitations.

Asymmetric Cryptography Services

- In asymmetric cryptography, services are distributed asymmetrically.
- Public keys normally available on a public key server.
- Anyone with access to your public key can encrypt information that only your private key can decrypt.
  - Confidentiality
- You (and only you) can encrypt information with your private key that anyone else can decrypt with your public key.
  - Authentication
  - Non-repudiation

Asymmetric Key Encryption Services

Confidentiality

- Sender encodes message with receiver’s public key.
- Receiver decodes with private key.

Authentication and Non repudiation

- Sender encodes message with sender’s private key.
- Receiver decodes with sender’s public key.

Asymmetric Algorithms

- RSA
  - Used for encryption and digital signatures
    - Most widely used asymmetric algorithm
- Diffie-Hellman
  - Allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
- El Gamal
  - Used in DSA, the Digital Signature Algorithm
    - Based on discrete logarithms
- Elliptic Curve
  - Economical in terms of computation, bandwidth, and storage
    - Finding the discreet logarithm in a finite field.
    - Optimum for use in small portable devices

Hybrid Cryptosystems

- Relative to classic cryptography, public key cryptography is slow.
  - 1,000 to 10,000 times slower than secret key cryptography.
- TypicalHybrid systems use public key crypto to distribute symmetric (session) keys.
  - Symmetric key for bulk data encryption
  - Asymmetric key for key distribution
- Will use one way functions to provide integrity
- Will use digital signatures to provide authentication and non repudiation

Diffie-Hellman Key Exchange

- Subjects exchange secret keys over an insecure comm channel without exposing the keys.
  - Introduced the notion of public key cryptography.
- Used for key distribution
- Not used to encrypt and decrypt messages.
  - OAKLEY: a key establishment protocol based on the Diffie-Hellman algorithm designed to be a compatible component of ISAKMP
    - Proposed for IPsec but superseded by IKE.
- Predates RSA.

RSA

- Public key algorithm derived from properties of large prime numbers.
  - In part, based on difficulty of factoring a number N, which is the product of two large prime numbers.
- Defacto standard for digital signatures and encryption.
  - At the time of its publication, Rivest, Shamir, and Addleman were all MIT Professors.
  - Issued in 1983, patent expired in 2000.

El Gamal

- Extended Diffie-Hellman concepts to apply to encryption and digital signatures.
- Non-patented public key cryptosystem based on the discrete logarithm problem.
- Used in free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems.

Elliptic Curve (EC) Cryptography

- Uses algebraic system defined on points of elliptic curve to provide public-key algorithms
- Smaller elliptic curve key sizes can yield higher levels of security.
  - Of all public key systems, highest strength per bit
- Requires less computational and memory requirements.
  - More suitable for small electronic devices

Elliptic Curve (EC)

- At a high level, Elliptic curve cryptosystems are analogs of existing public-key cryptosystems in which modular arithmetic is replaced by operations defined over elliptic curves.
- Can be classified into two categories according to whether they are analogs to RSA or discrete logarithm based systems.

One Way Problems and Functions

- A function that is simple to evaluate but is difficult to invert is called a one way function.
- If there is a hidden shortcut that simplifies the otherwise difficult inverse process, then one speaks of a trapdoor function.

Example problems include:

- Discrete logarithm problem

  $F(x)=a^x(mod n)$
- Product of two large prime numbers (Factorization problem)

  $PxQ=N$,

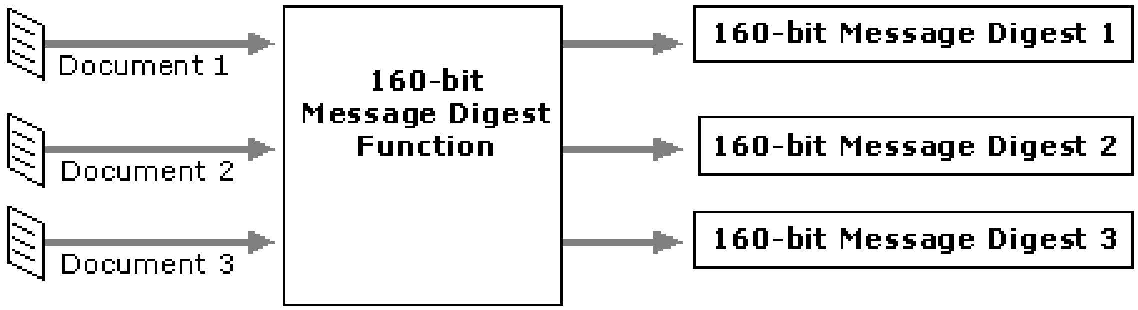
  given N it is difficult, for large primes, to discover P and Q

One Way Problems and Functions

- In a similar, but different, manner a hash is also a one way function.
  - A hash function though is irreversible.
  - A hash function takes a variable length input and produces a fixed length output (the hash).
  - A small change in input should produce a significant change in output.
  - It must be difficult for an attacker to produce a collision
    - A collision is where different inputs produce the same hash.

One Way Functions

- Hash: One way function that provides message integrity services.



- May also be called a message digest, message integrity check (MIC), digital fingerprint, or similar term.

Message Digest Attributes

- Original file cannot be created from message digest (one way function).
- Given a file and its corresponding message digest, it should not be feasible to find another file with the same message digest.
  - Called a collision
  - Could be strongly or weakly collision resistant
    - See birthday attack
- Should be calculated using all of the original file's data.

SHA-1

- When any message less than 2^{64} bits is input, SHA-1 produces a unique 160 bit message digest.
- Any modifications to the message being sent to the receiver results in a different message digest being calculated by the receiver.
- NSA developed.
  - Evolution of MD4.

MD5

- Message digest algorithm.
  - IETF standard (RFC 1321)
  - Developed by Rivest in 1991.
  - Used in PGP.
- Generates a 128 bit message digest from an arbitrary length text.
- Recent papers have pointed to weaknesses in some hashes including MD5. See:

http://www.cryptography.com/cnews/hash.html

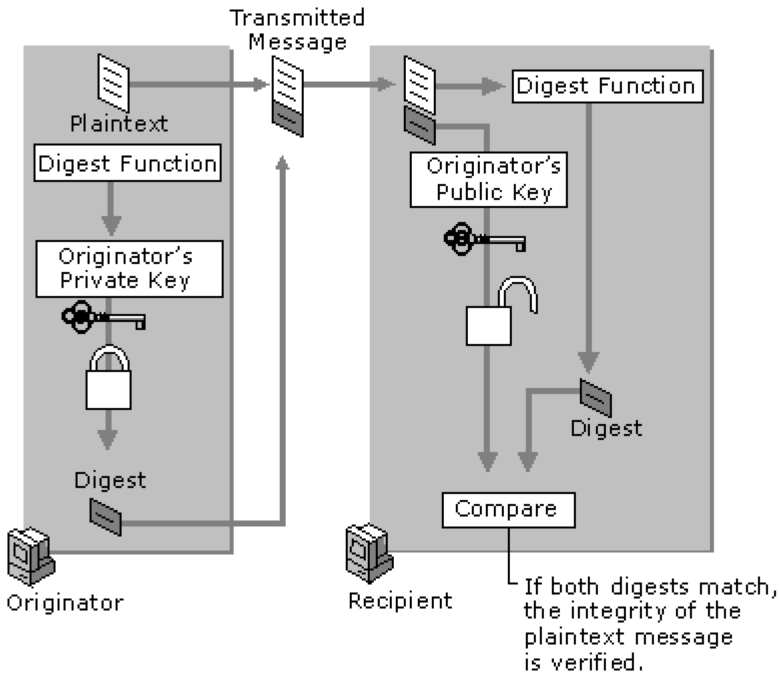
HMAC

- Key dependent hash function.
- Creates a Message Authentication Code (MAC) bound to both the message and the shared symmetric key.
  - Prior to hashing, concatenates symmetric key with message.
  - Authentication and integrity services.
- HMAC, with SHA-1 [FIPS-180-1], provides an authentication mechanism within the revised IPSEC Encapsulating Security Payload [ESP] and the revised IPSEC Authentication Header [AH].
  - RFC-2104

RSA Digital Signature

- A document hash encrypted with a sender's private key is called a digital signature.
- Digital signatures bound to both:
  - Document and
  - Signer
- The receiver decrypts the message digest with the sender's public key.
  - If the public key opens the message digest, the senders identity is verified. (nonrepudiation)
- The receiver can re-compute the message digest.
  - If the value of the hash hasn't changed, the message has integrity.

RSA Digital Signatures



- First create a fixed length Message Digest.
- Then, encipher the digest with the senders private key.
- Process binds the fixed length block to:
  - The original data
  - The sender.

Digital Signature Standard (DSS) and Secure Hash Standard (SHS)

- Both digital signature algorithms use the Secure Hash Algorithm (SHA-1).
  - Defined in NIST's FIPS 180.
- A message digest is then processed by the DSA to either generate or verify a signature.
- DSA is based on the discrete logarithm problem.
- Can also be implemented with elliptic curves

Digital Signature Technologies Compared

- RSA can both encrypt and sign. In contrast, DLSSs can only sign.
- DLSSs need to generate random numbers for each signature.
- DLSS can provide the same level of security with a smaller key.
- RSA is faster.

Questions?

References One:

http://cis.gsu.edu/~rbaskerv/cis8680/Lessons/crypto/index.html

http://www.simonsingh.net/Crypto_Corner.html

http://www.schneier.com/

http://www-106.ibm.com/developerworks/library/s-pads.html

http://www.math.temple.edu/~renault/cryptology/affine.html

References Two

https://www.isc2.org/cgi-bin/request_studyguide_form.cgi?AG=6042

http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/distsys/part2/dsgch14.mspx

http://www.fas.org/irp/nsa/rainbow.htm