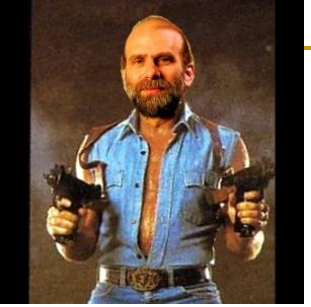
Applied Cryptology

Ed Crowley

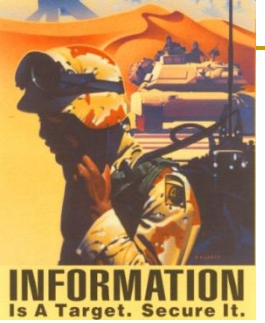
Topics

- Basics
  - Basic Services and Operations
- Symmetric Cryptography
  - Encryption and Symmetric Algorithms
- Asymmetric Cryptography
  - Authentication, Nonrepudiation, and Asymmetric Algorithms
- One way functions
  - Integrity and Hashing
- Digital Signatures
- PKI



Basics

- Cryptography refers to the science and art of designing ciphers
  - Currently defined as a branch of Mathematics
- Cryptanalysis refers to the science and art of breaking ciphers
- Cryptology, often shortened to crypto, refers to the study of both



Basic Crypto Services

1. Confidentiality – Deals with who can read data
2. Integrity – Deals with who can write data.
3. Authentication – Deals with having proof of whom, or what, with which you are interacting
   - When Bob receives a message that purports to be sent by Alice, Bob can be sure that the message was really sent by Alice.
4. Nonrepudiation
   - Alice cannot later deny that the message was sent.
   - Bob cannot later deny that the message was received.
   - Third party verifiable

Note: cryptography not concerned with availability.

Basic Crypto Operations

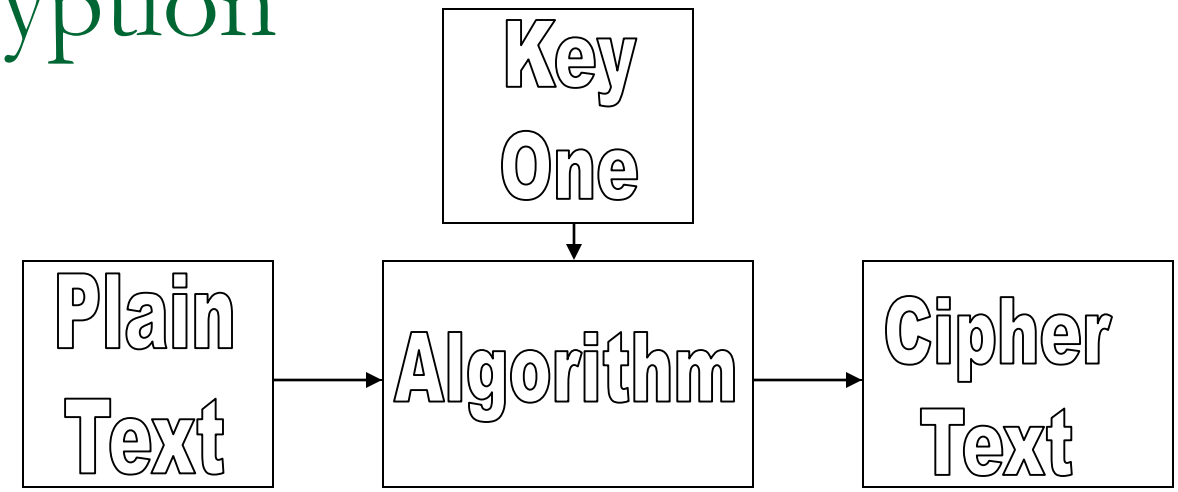
- Symmetric Crypto *(aka single key or classic)*
  - Block or stream
- Asymmetric Crypto *(aka two key or key pair)*
  - Problem hard one way, easy another…
- One-way functions
  - Integrity
- Most cryptosystems utilize multiple basic operations aka are Hybrid Cryptosystems
  - For example, PKI combines all 3 operations.
  - Digital Signatures combine Single and Two key…

Practical Systems Combine Operations aka Hybrid Cryptosystems

- Hybrid systems combine multiple basic operations, potentially including:
  - Symmetric
  - Asymmetric
  - One way.
- For example, in SSL the servers public key, from it's certificate, encrypts a temporary symmetric session key while a one way operation provides integrity.

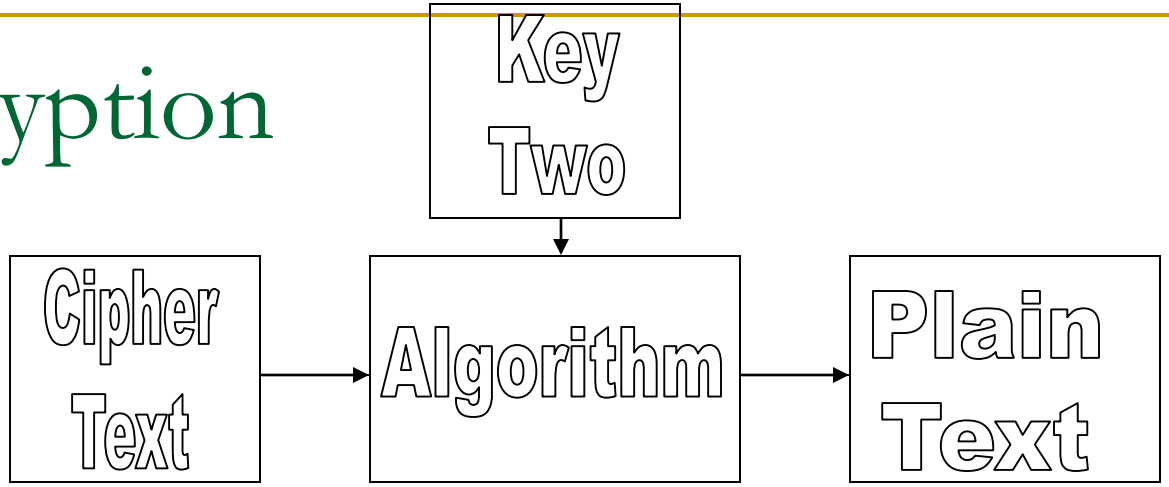
Lets look at Encryption.

Encryption



- Two inputs
  - Key One and plain text are inputs to encryption algorithm.
- One output
  - Cipher text which can be sent over an unsecure medium…

Decryption



- Likewise, two inputs, one output
  - Key Two and cipher text are inputs.
- One Output: Plain Text.
  - Symmetric crypto, Key One and Key Two identical.
  - Asymmetric crypto, Key One and Key Two, related but different.

… ciphers may either have one key for both encryption and decryption, in which case they're called shared key (also secret key or symmetric), or have separate keys for encryption and decryption, in which case they're called public key or asymmetric.

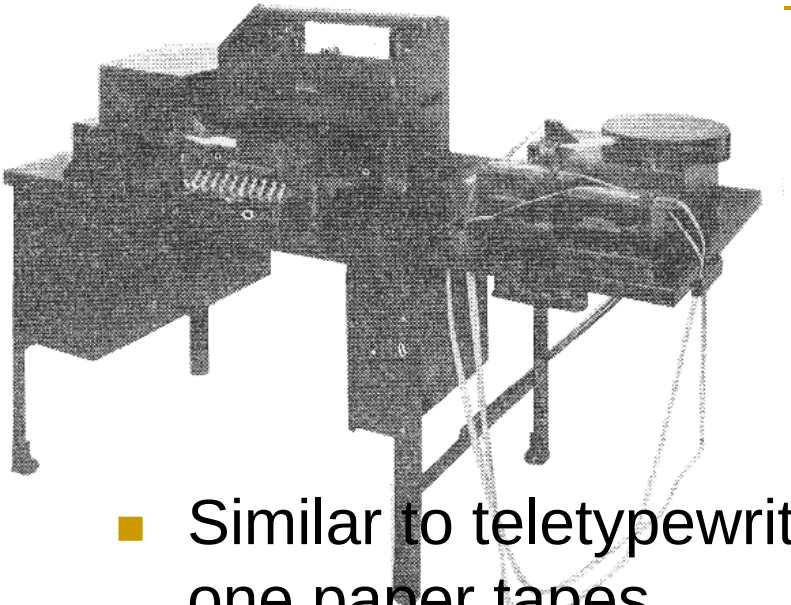
--Ross Anderson

Kerckhoff's Principle aka Shannon's Maxim

- All security is in the key (aka the enemy knows/has the system)
  - With large key sizes, can be very strong.
    - In this context, strong symmetric crypto refers to key sizes 128 or more bits
  - Key compromised? No security.
- Consequently, key management is critical
  - And in Symmetric Crypto, key management is a problem

Symmetric Crypto Attributes

- Variety of algorithms…
  - Each of which can run in a variety of modes …
- Symmetric Algorithms classified as either stream or block
  - Block algorithms further classified by:
    - Key length
    - Block size
- Fast.
  - Bulk encryption almost always implemented with symmetric crypto…
- Given enough time and enough resources, brute force attack will always succeed.(NTIM)

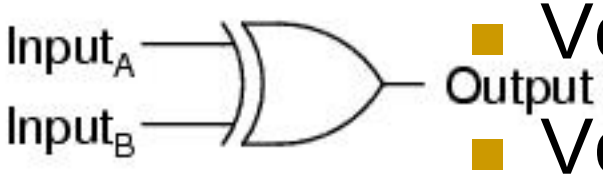


1914 Vernam Stream Cipher Machine

- Similar to teletypewriter except that it used three rather than one paper tapes .
  - First tape, sender types a message in the form of holes and spaces. (plain text)
  - Second tape, contains random characters. (key)
- Cipher Machine combines the holes and spaces of the message tape with the holes and spaces of the random-character tape using Modulo-2 (XOR).
  - This produced the third tape containing the enciphered message (cipher text).
- Cipher text then be transmitted and saved on a paper tape.

Exclusive Or (XOR)

Exclusive-OR gate



- Very easy hardware implementation.
- Very fast hardware implementation.

Reversible

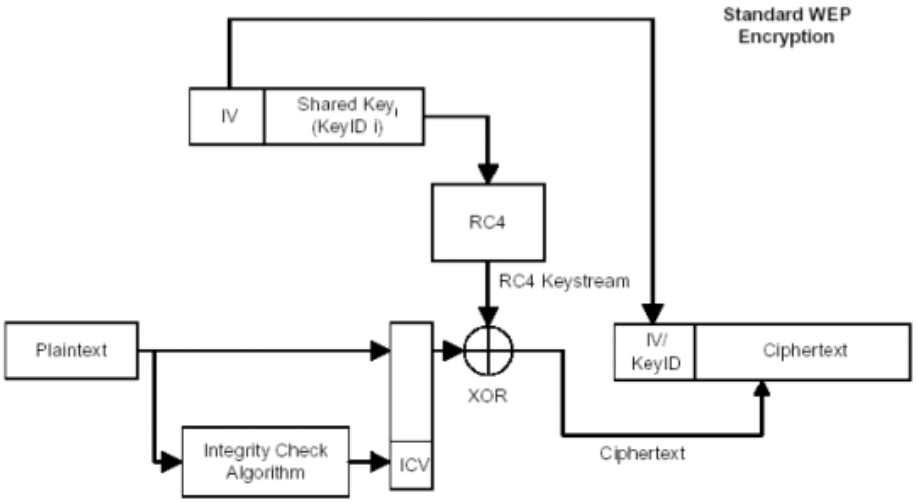
- Plain text + Key = Cyphertext
- Cyphertext +Key= Plaintext

A	B	Output
0	0	0
0	1	1
1	0	1
1	1	0

Frequently used to implement stream ciphers.

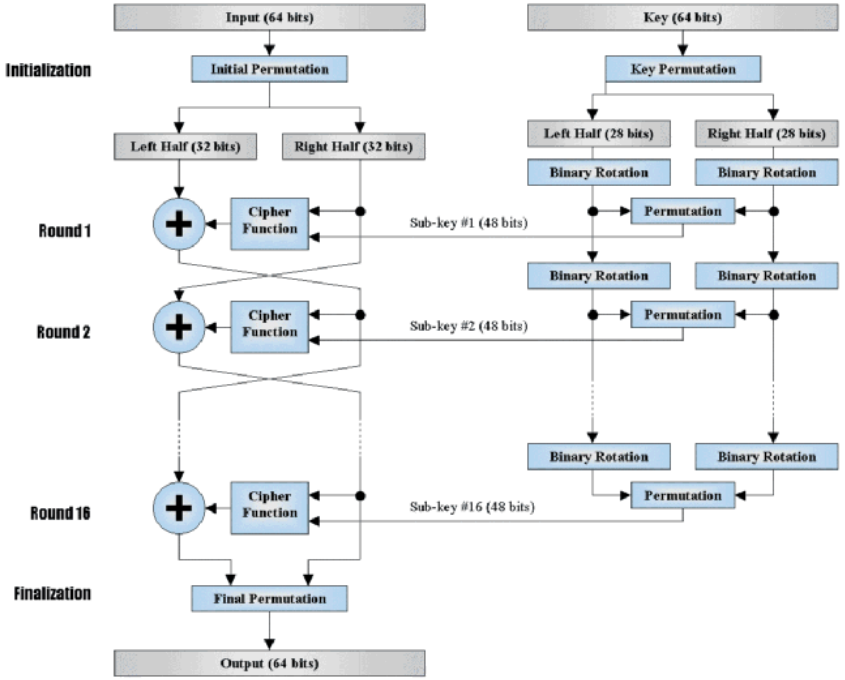
Symmetric Ciphers

- RC-4 (Rivest Cipher 4) Fast symmetric streaming cipher used in a variety of implementations
- DES Former US Standard originally based on IBM's and Horst Feistel's Lucifer algorithm.
- Triple DES Temporary US Standard designed to response to brute force attacks against DES
- AES US National Encryption Standard for other than Top Secret



RC-4 Stream Cipher (WEP)

- Both Vernam and RC-4 are stream ciphers.
- Typically, stream ciphers are designed for hardware implementation.



DES Block Cipher

- In contrast, DES is a block cipher.
- Typically, block ciphers are designed for software implementation.
  - Operates on 64 bit blocks.

One Cipher to Rule them All!

One Time Pad

- Special Vernam Cipher implementation where:
  - Key and message same length.
  - Key totally random.
  - Key used only one time for only one message.
  - Key securely distributed
- Done properly, creates an unbreakable cryptosystem.
  - Only cipher mathematically provable unbreakable.
- Considered by many impossible to do in a large scale real world implementation.
  - *See NSA's Venona project.*

http://www.pro-technix.com/information/crypto/crypto_frame.html

Symmetric Key Algorithms: DES

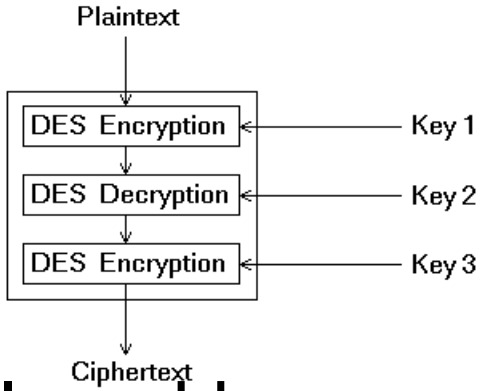
- First modern, secure symmetric encryption algorithm.
- Significant attributes:
  - Known in great detail
  - Free from patent issues
- Relatively simple, uses only three functions
  - XOR
  - Permutation
  - Substitution
- Originally, designed for hardware implementation

Single DES Weaknesses

- Relatively short, 56 bit, fixed key length with a fixed 64 bit block length
  - Designed for ’70s era Hardware implementation
- 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.

Triple DES (3DES)

- Original temporary DES replacement .
  - Effective 168 bit key length
    - 3X56
    - Implemented with 2 or 3 keys



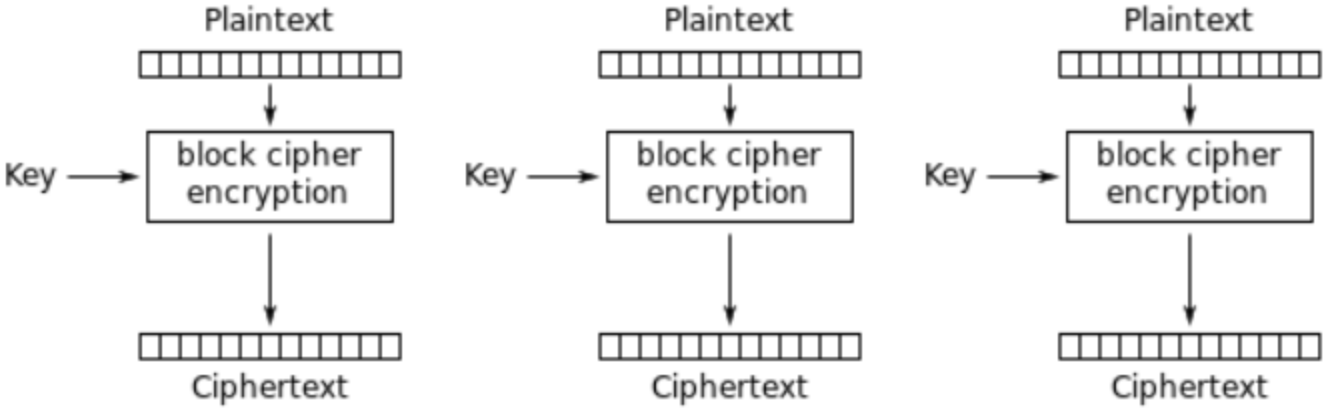
- As FIPS Standard, DES was replaced by AES (Advanced Encryption Standard)
  - Note: *NIST Federal Information Processing Standard (FIPS) 140 sets standards for cryptographic modules.*

DES Modes of Operation

- A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block.
- A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block

Electronic Codebook (ECB) Mode

- Message divided into blocks. Each block encrypted separately.

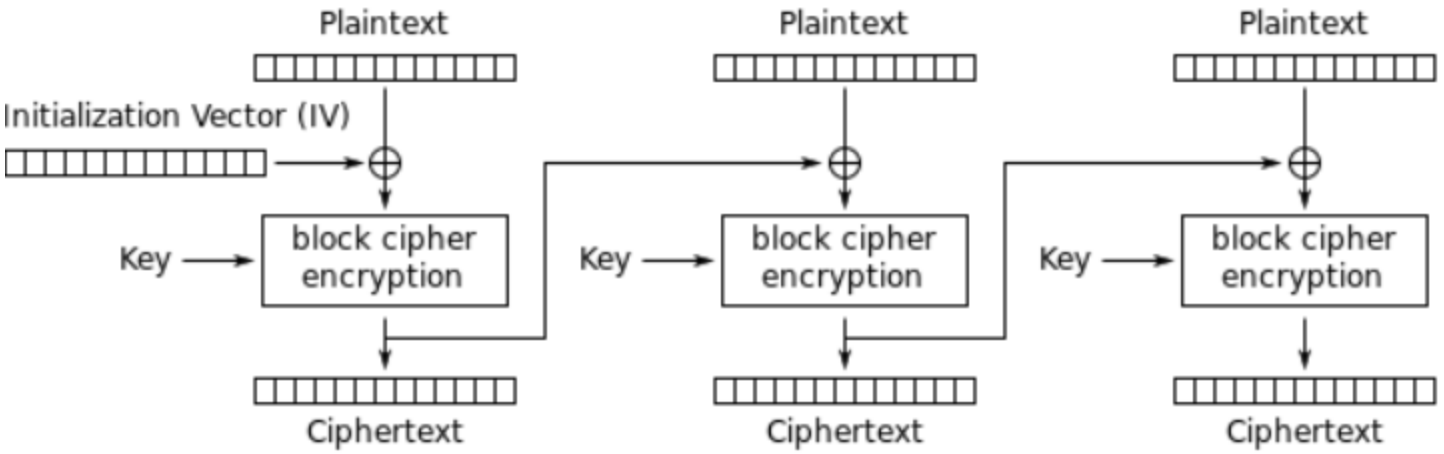


Electronic Codebook (ECB) mode encryption

- Disadvantage: plaintext blocks encrypted into identical ciphertext blocks.

Cyber Block Chaining Mode

- Each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point.

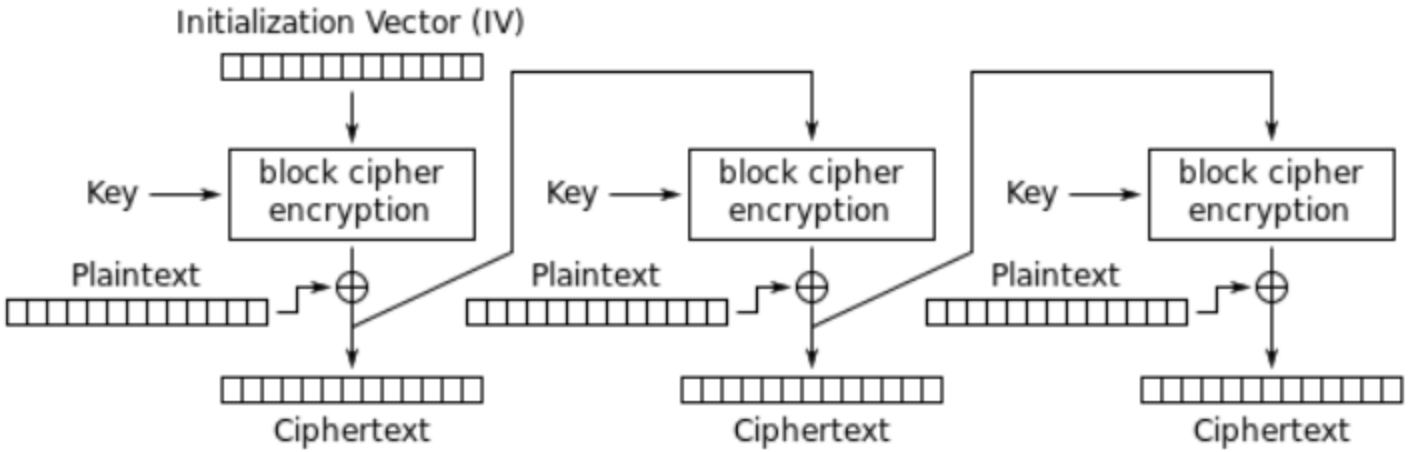


Cipher Block Chaining (CBC) mode encryption

- Most commonly used mode of operation

Cipher Feedback (CFB) Mode

- Makes a block cipher into a self-synchronizing stream cipher.

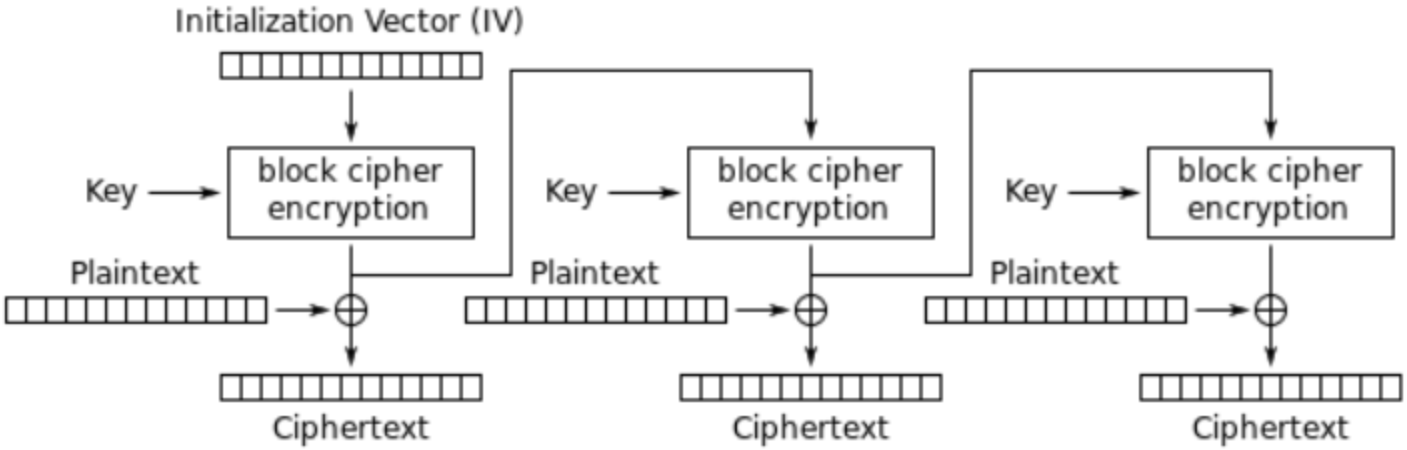


Cipher Feedback (CFB) mode encryption

- Message does not need to be padded to a multiple of the cipher block size

Output Feedback (OFB) Mode

- Makes a block cipher into a synchronous stream cipher.



Output Feedback (OFB) mode encryption

- Each output feedback block cipher operation depends on all previous ones, and so cannot be performed in parallel.

Advanced Encryption Standard (AES)

- AES, aka Rijndael Block Cipher
- Utilizes variable 128, 192, 256 bit length key with a 128 bit block size.
- Replaced DES/3-DES.
  - Announced January 1997.
  - Current Federal Information Processing Standard (FIPS) Standard
  - US standard for protection of sensitive but unclassified information.

(Symmetric) Key Management Problem

- Issues include:
  - Only works by prearrangement.
    - Recipient must already posses key.
  - How do you deliver key 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.
- Doesn't scale well.
  - A system with N users requires (N*(N-1))/2, keys
- Key Management problem led to the creation of Asymmetric Cryptography

Asymmetric Cryptography

- Utilizes mathematically related key pairs
  - One key public, one key private
  - Asymmetric private key is never shared.
- Keys based upon problems that are easy to solve one way but 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
- Offers solution to Symmetrical Cryptography Key Management problems.

Symmetric/Asymmetric Technologies Compared

- Symmetric key
  - Single shared secret key.
    - AKA secret key, private key, single key, or classic cryptography.
  - Fast
- Asymmetric key
  - Two different, but related, keys
  - One key public. One key private (secret)
    - AKA public key or two key cryptography.
  - Slow. Not usually used for bulk encryption

Asymmetric Algorithms

- RSA
  - Used in hybrid crypto systems for encryption and digital signatures
    - Most widely used asymmetric algorithm
- 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
- Diffie Hellman key exchange protocol
  - Allows two entities to jointly establish a shared secret key over an insecure communications channel

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.

Potential Asymmetric Crypto Services

Confidentiality

- Sender encodes message with receiver's public key.
- Receiver decodes with private key.
  - Only short messages, typically shorter than key.

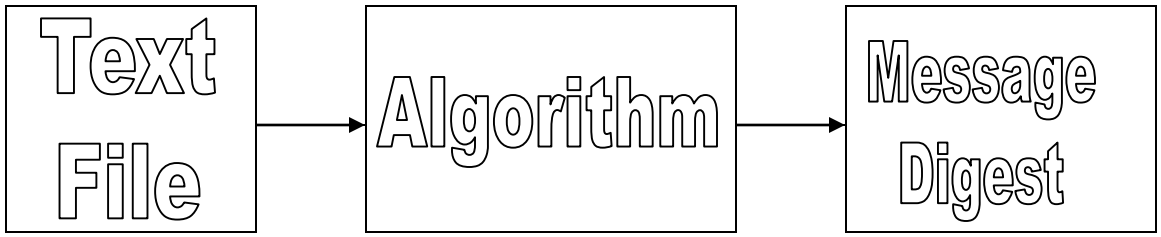
Authentication and Non repudiation

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

Authentication and NonRepudiation

- Authentication verifies that a message came from whom it is represented to come from.
- Non repudiation provides evidence so that a message can not be disavowed at a later time.
  - Process utilizes a secret known to only one person (private key).
  - Methods include digital signatures.

One Way Process: Integrity



- A Hash, or message digest, enables you to discern whether or not a document has been altered.
  - That is, it proves or disproves data integrity.
  - A hash is considered bound to a document.
    - Sometimes called a digital fingerprint.
- Hashes can also be components of digital signatures and Message Authentication Codes (MACs).
  - The above drawing illustrates a keyless hash process.
    - However, there are also keyed integrity processes called message authentication codes (MACs or HashMACs).

Message Digests (Hash)

- Message digest 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. Message Integrity Code or MIC
   1. Bound just to original document
2. Message Authentication Code or MAC
   1. Bound to original document and sender (by a shared secret key)

[1.] H.X. Mel

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

- 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.

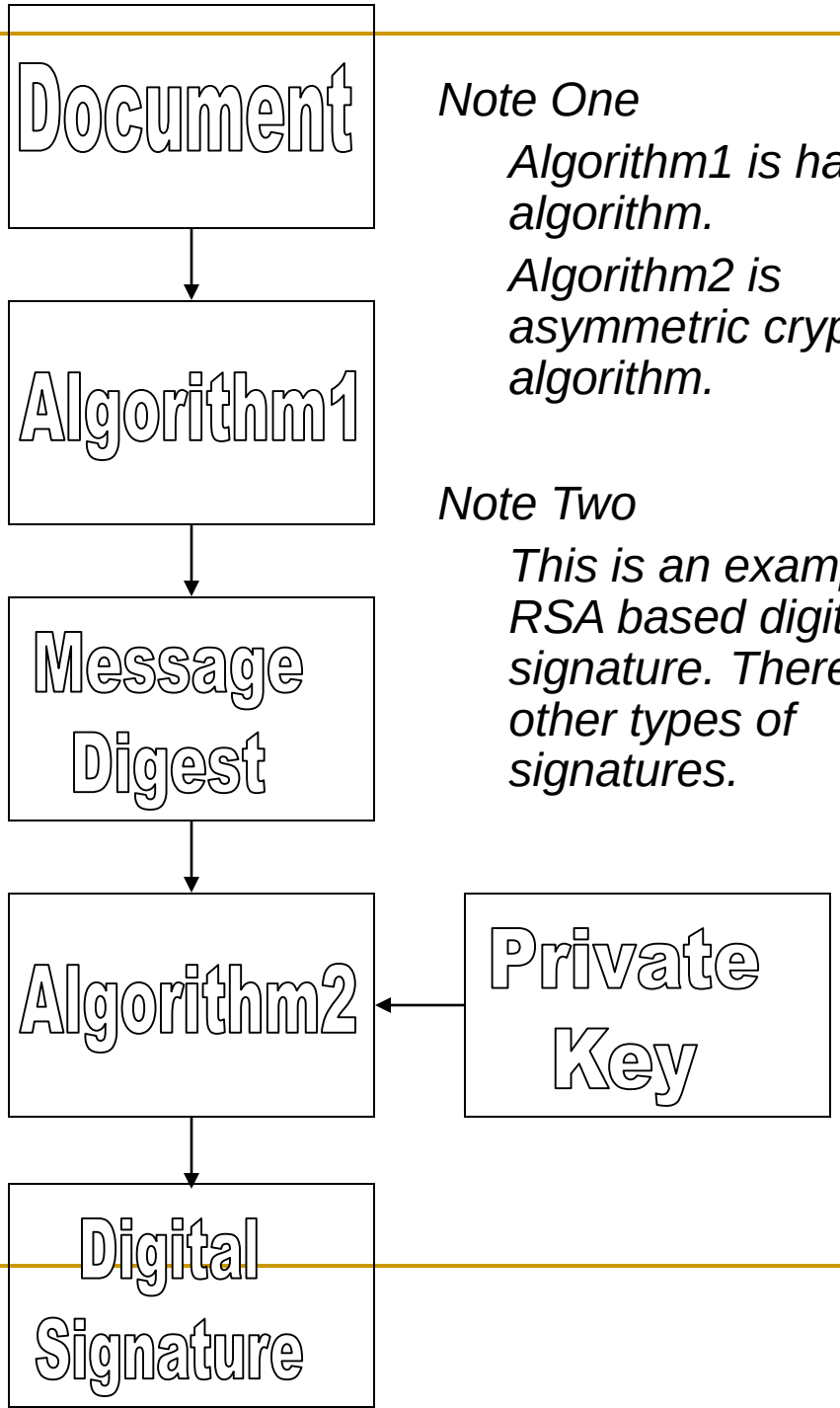
MD5

- 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

RSA Digital Signature Creation

1. Hash document to create digest
2. Encrypt hash with senders private key
3. Attach to encrypted hash communication
4. Upon delivery, recipient decrypts hash with senders public key
5. Creates new document hash and compares
6. If hashes are identical, documents have integrity.



Note One

Algorithm1 is hash algorithm.

Algorithm2 is asymmetric crypto algorithm.

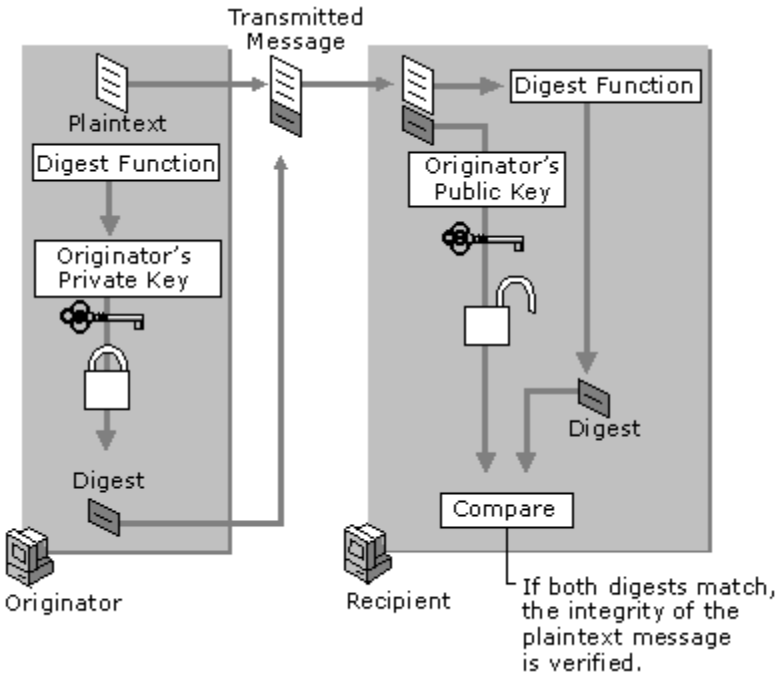
Note Two

This is an example of an RSA based digital signature. There are other types of signatures.

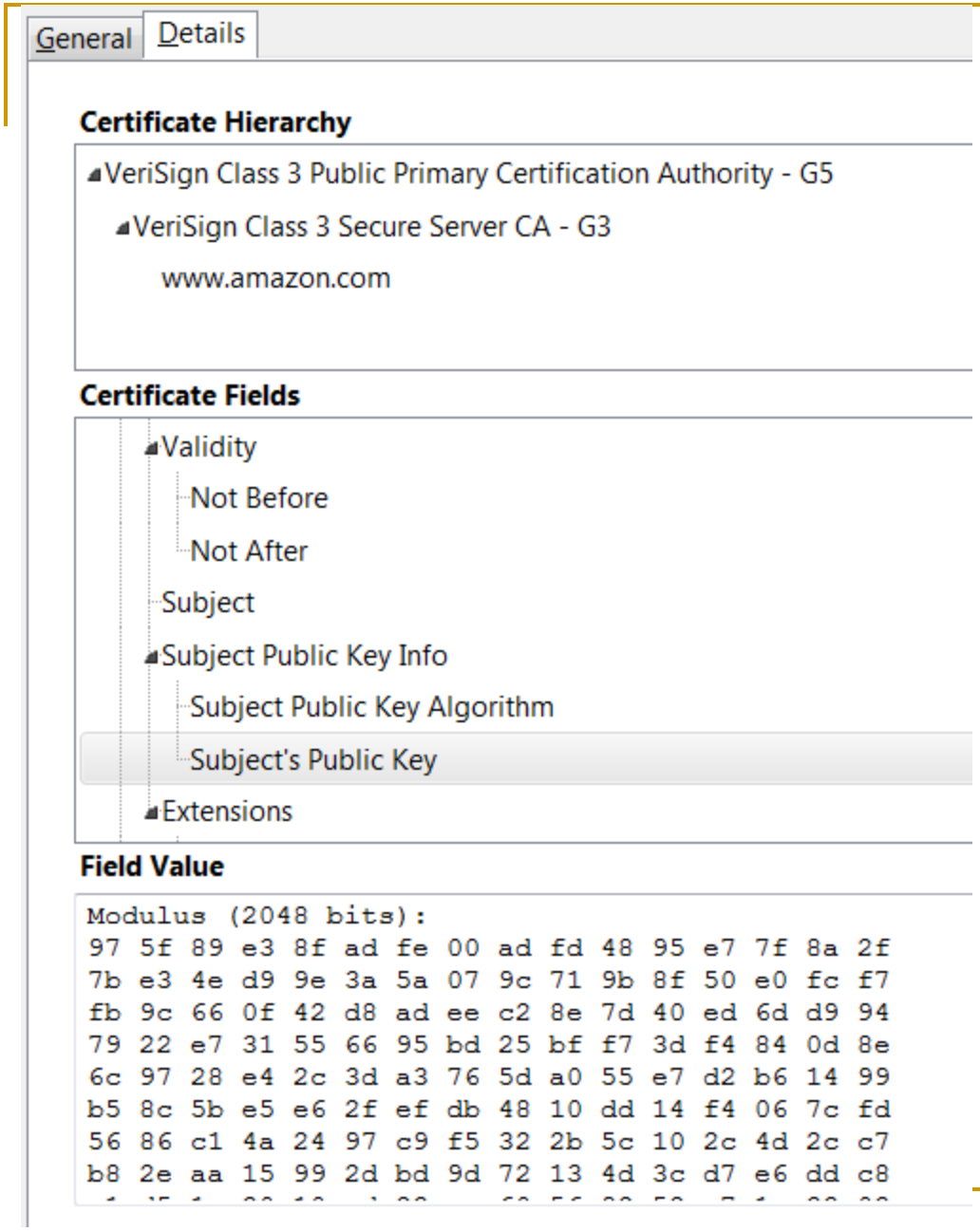
RSA Digital Signature

- 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 Again



- 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.



- Certificate binds an entitie's public key to the entity.
- In instant case, Amazon is bound to the public key on the left.

Questions?

Selected References

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