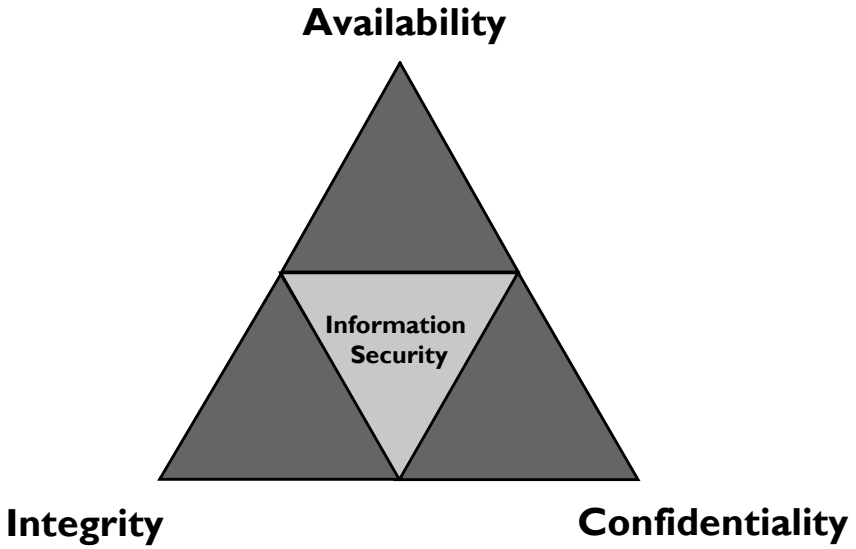
Cryptography

Domain Objectives

- Basic Cryptographic Concepts
- Cryptographic Algorithms and Uses
- Message Integrity Codes
- Digital Signatures
- Certification
- Cryptanalysis

Information Security TRIAD



Domain Agenda

- **Introduction**
- Cryptography
  - Introduction to Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Message Integrity Controls
  - Key Management
  - Uses of Cryptography
  - Legal Issues
- Cryptanalysis
- Information Hiding Techniques

Historical Development of Cryptography

- Cryptographic Techniques
  - Manual 
  - Mechanical 
  - Electro-mechanical 
  - Electronic 
  - Quantum Cryptography 

Basic Goals of Cryptography

- Ensure confidentiality of sensitive information
- Ensure integrity of information
- Verify the authenticity of communications
- Provide measures to support non-repudiation
- Provide foundation for secure access control
- Make compromise too expensive or too time-consuming

Domain Agenda

- Introduction
- Cryptography
  - **Introduction to Cryptography**
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Message Integrity Controls
  - Key Management
  - Uses of Cryptography
  - Legal Issues
- Cryptanalysis
- Information Hiding Techniques

Key Concepts and Definitions

- Cryptography 
- Cryptanalysis 
- Cryptology 

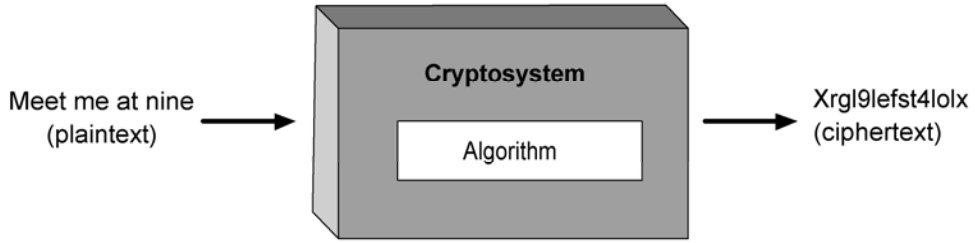
Key Concepts and Definitions

- Plaintext/Cleartext
- Ciphertext/Cryptogram
- Encipher/Encrypt/Encode
- Decipher/Decrypt/Decode

Key Concepts and Definitions

- Cryptographic Algorithm
- Cryptosystem
- Cryptovariable (Key)
- Key Space

Key Concepts and Definitions



Basic Cryptosystems

- Codes
- Simple Substitution Ciphers
- Simple Transposition Ciphers
- Polyalphabetic Ciphers
- Running Key Ciphers
- One-Time Pads

Codes

- Encoding words and phrases
- For simplifying transmission of basic secrecy and integrity
  - Colored Flags for Navy Ships (Telegraphy)
  - Morse Code

Simple Transposition Ciphers

- Disguising a message by rearranging the letters or bits in the message
  - Plaintext "This is an example of transposition"
  - Cipher "tsaoni hamfst inptpi selroo ixeasn"
- Multiple ways to produce ciphertext

T	H	I	S	I
S	A	N	E	X
A	M	P	L	E
O	F	T	R	A
N	S	P	O	S
I	T	I	O	N

Simple Substitution Ciphers

- Based on the substitution of one value for another
  - Shift Alphabet (move letters 3 spaces)
    - A B C D E F ..... FACE
    - D E F G H I ..... IDFH
  - Scramble Alphabet (substitute one letter for another)
    - A B C D E F ..... FACE
    - Q E Y R T M ..... MQYT

Polyalphabetic Ciphers

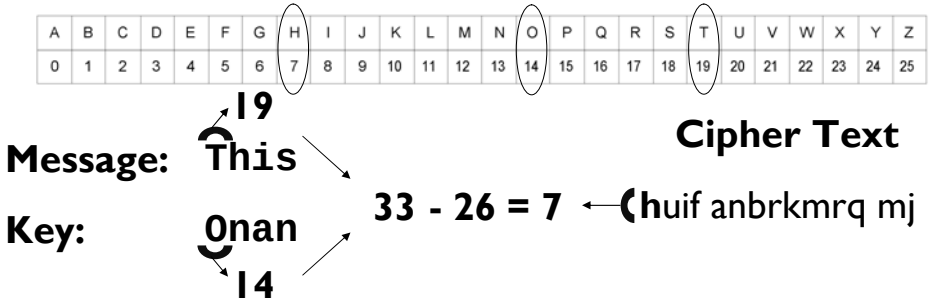
- Substitution cipher using multiple alphabets

	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
1	Z	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
2	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
3	X	W	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
4	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
...																										

Encrypt the plaintext word 'FEEDBACK' using a key of 3241.

Running Key Ciphers

- Encryption through use of the numerical value of letters in the plaintext and a shared book
  - Key: 'On a non interfering basis over …'
  - Message: 'This material is enciphered'



One-Time Pads (OTP)

- Originator and receiver have same pad of key values
- Each key is used once only and then discarded
- Only unbreakable algorithm

Making Secure Cryptographic Algorithms

- Simple cryptosystems are not very secure
  - Discernible
  - Redundancies and statistical patterns in natural language
- Claude Shannon identified two key characteristics
  - Confusion
  - Diffusion

Basic Transformation Techniques

- Substitution
- Transposition or Permutation
- Compression
- Expansion
- Padding
- Key Mixing
- Initialization Vectors (IV)
- Exclusive-Or (XOR)

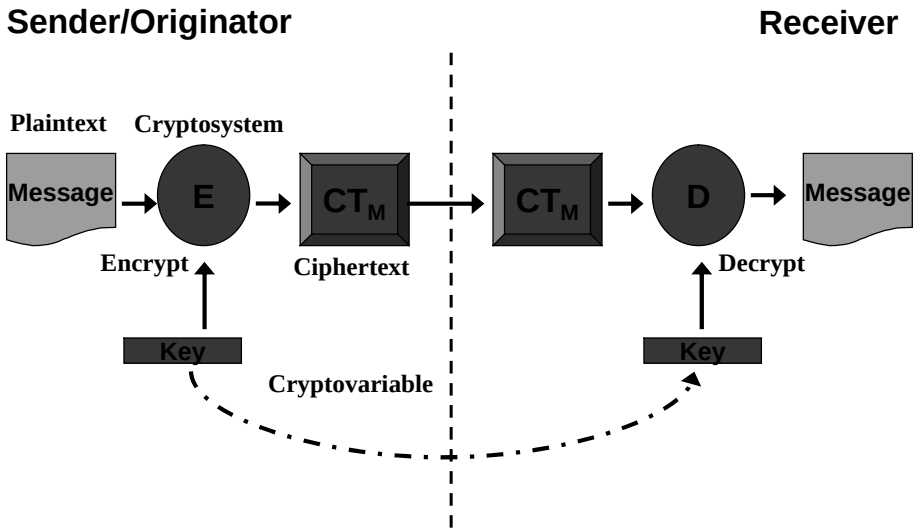
Domain Agenda

- Introduction
- Cryptography
  - Introduction to Cryptography
  - **Symmetric Key Cryptography**
  - Asymmetric Key Cryptography
  - Message Integrity Controls
  - Key Management
  - Uses of Cryptography
  - Legal Issues
- Cryptanalysis
- Information Hiding Techniques

Symmetric Key Cryptography

- Single Shared Key
- Many Algorithms
- Two Main Classes
  - Stream Ciphers
  - Block Ciphers

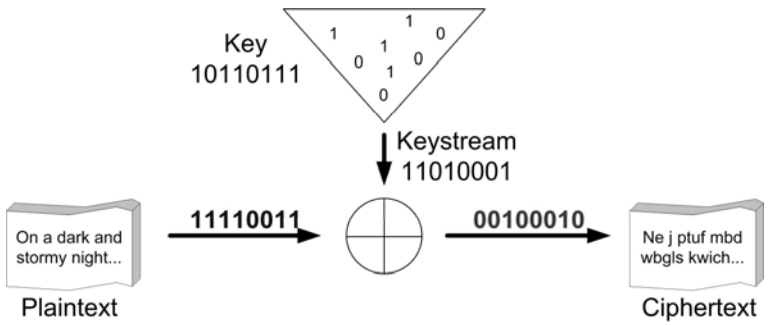
Basic Symmetric Key Cipher Operation



Stream Ciphers

- Keystream
  - Statistically Unpredictable and Unbiased
- Operates on individual bits

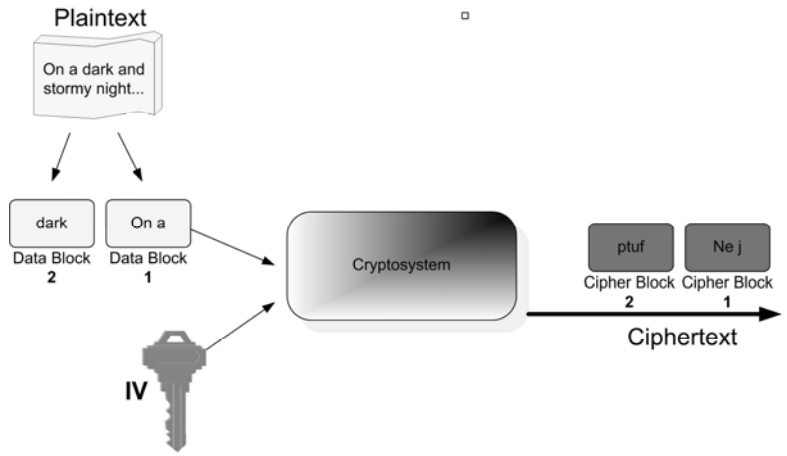
Stream Cipher Operation



Block Ciphers

- Fixed-sized Blocks
- Plaintext XOR'ed with Cipher Blocks
- Sensitive to Small Changes/Errors

Block Cipher Operation



Data Encryption Standard (DES)

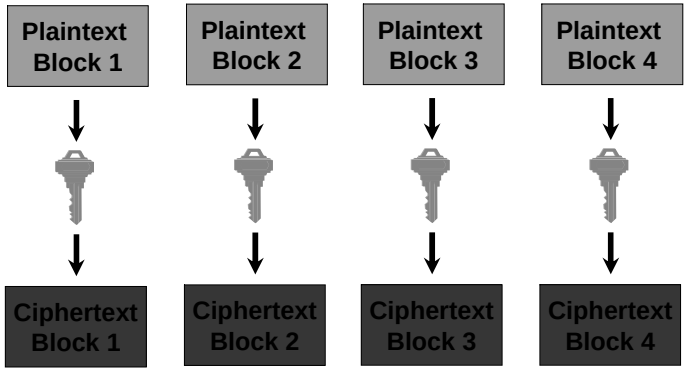
- Designed by IBM
- Optimized by US National Security Agency (NSA)
- 64-bit block size
- 56-bit true key plus 8 parity bits
- 16 rounds

Modes of DES

- Block Modes
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
- Stream Modes
  - Cipher Feed Back (CFB)
  - Output Feed Back (OFB)
  - Counter (CTR)

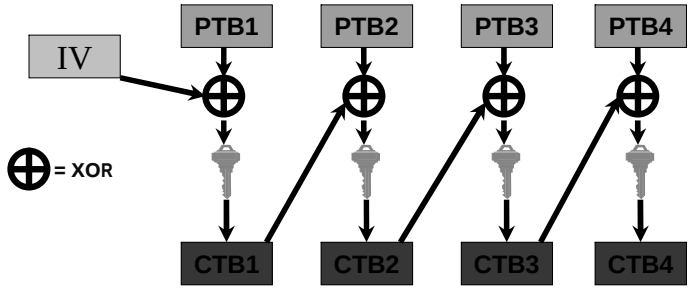
Electronic Code Book (ECB)

- Each block of plaintext is encrypted independently using the same key



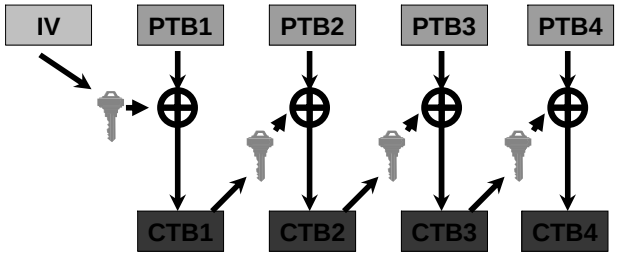
Cipher Block Chaining (CBC)

- First block of plaintext is XOR'ed with an Initialization Vector
- Next plaintext block, the cipher text result of the previous operation is used in place of the IV



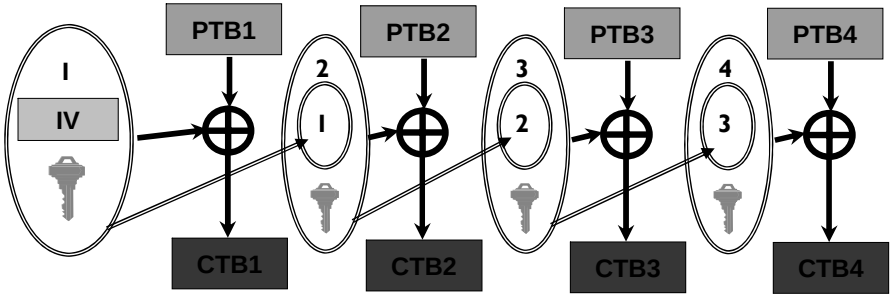
Cipher Feed Back (CFB)

- Similar to CBC except that IV is encrypted and then the result is XOR'ed with the first plaintext block
- For the next plaintext block, the cipher text result of the previous operation is used in place of the IV



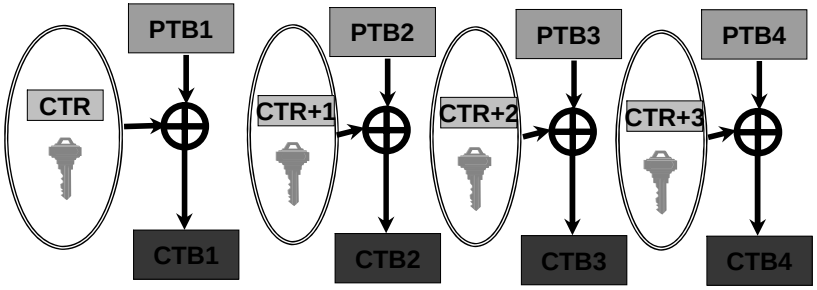
Output Feed Back (OFB)

- Operates very much like CFB
- Except that only the RESULT of the first step (encrypting the IV) is fed back into the next operation



Counter (CTR)

- Operates very much like OFB
- Except that a counter value is used instead of an IV



Summary of Block Cipher Modes

Mode	Block / Stream Mode	Long / Short Messages	Serial / Parallel operation possible	Effect of an error	Work that can be done in advance
ECB	Block	Short	Fully parallel	Contained	Keys
CBC	Block	Long	Fully serial	Contained	Keys and IV
CFB	Stream	Long	Fully serial	Contained	Keys and IV
OFB	Stream	Long, but errors are a problem	Partially serial and parallel	Cascades	Most encryption
CTR	Stream	Long	Fully parallel	Contained	Most encryption

DES

- Double DES (DDES)
- Triple DES (TDES)
  - DES-EEE3 or 3TDES-EEE
  - DES-EDE3 or 3TDES-EDE
  - DES-EEE2 (2TDES-EEE), DES-EDE2 (2TDES-EDE)

International Data Encryption Algorithm (IDEA)

- Published in 1991 as a replacement for DES
- Highly optimized for general-purpose computers
- 64-bit input and output block size
- 128-bit key (no parity bits)
- Basic operation is 8 rounds

AES (Rijndael)

- Rijndael algorithm originally published in 1998
- Block size
- Variable number of rounds

Other Examples of Block Ciphers

- RC5
- RC6
- Blowfish
- Twofish
- CAST
- SAFER
- Serpent

Strengths of Symmetric Key Cryptography

- Very fast
- Very difficult to break cipher text
- Algorithms and tools are freely available
- Stream ciphers are highly efficient
- Block ciphers offer multiple modes

Weaknesses of Symmetric Key Cryptography

- Key Negotiation / Exchange / Distribution
- Poor Scalability
- Limited Security

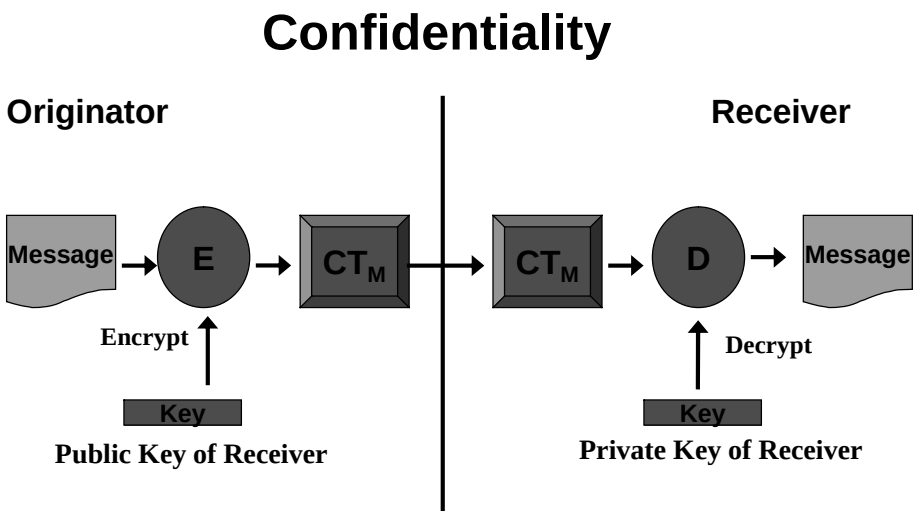
Domain Agenda

- Introduction
- Cryptography
  - Introduction to Cryptography
  - Symmetric Key Cryptography
  - **Asymmetric Key Cryptography**
  - Message Integrity Controls
  - Key Management
  - Uses of Cryptography
  - Legal Issues
- Cryptanalysis
- Information Hiding Techniques

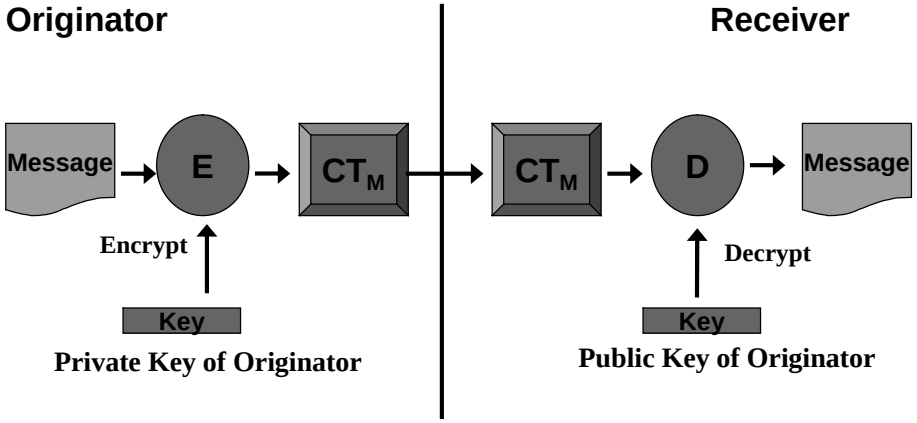
Asymmetric Key Cryptography

- Also known as public key cryptography
- Uses a pair of mathematically-related keys
  - Private Key
  - Public Key
- Introduced by Diffie and Hellman in 1976

Public Key Algorithms

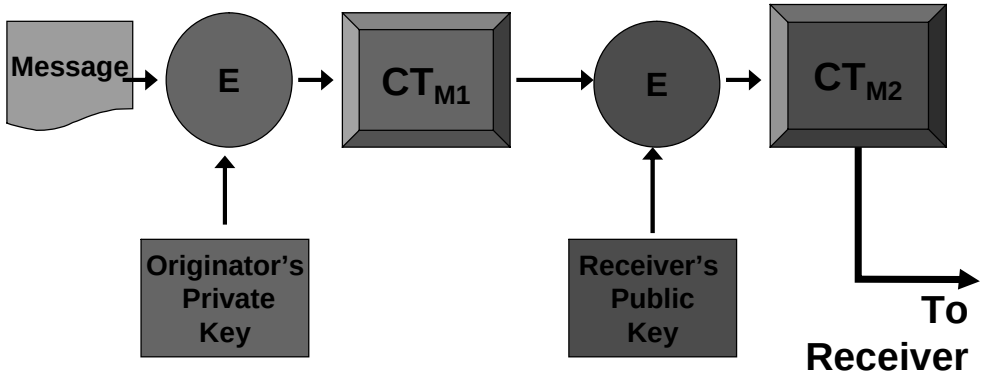


Proof of Origin



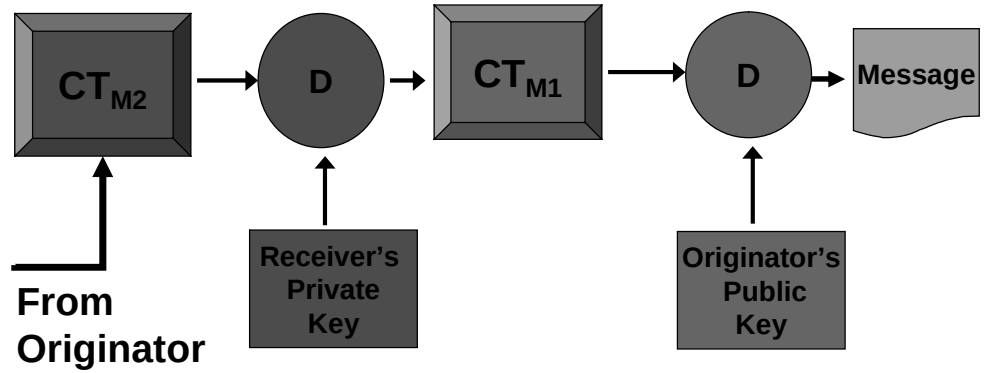
Confidentiality and Proof of Origin

Originator's Perspective



Confidentiality and Proof of Origin

Receiver's Perspective



- Factoring the product of two large prime integers
- Discrete logarithms in a finite field

Rivest-Shamir-Adleman (RSA) Algorithm

- Public-key cryptosystem that offers encryption, key distribution for symmetric keys and digital signature services
- Developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977
- Adjustable Keysize

Other Asymmetric Key Cryptographic Algorithms

- Diffie-Hellman Key Exchange Protocol
- ElGamal
- Elliptic Curve Cryptography (ECC)
- Merkle-Hellman Knapsack
- Chor-Rivest Knapsack

Asymmetric Key Cryptography

- Strengths
  - Confidentiality/Privacy
  - Access Control
  - Authentication
  - Integrity
  - Non-repudiation
- Weaknesses
  - Computationally Intensive
  - Slow (1000 or more times slower than symmetric)

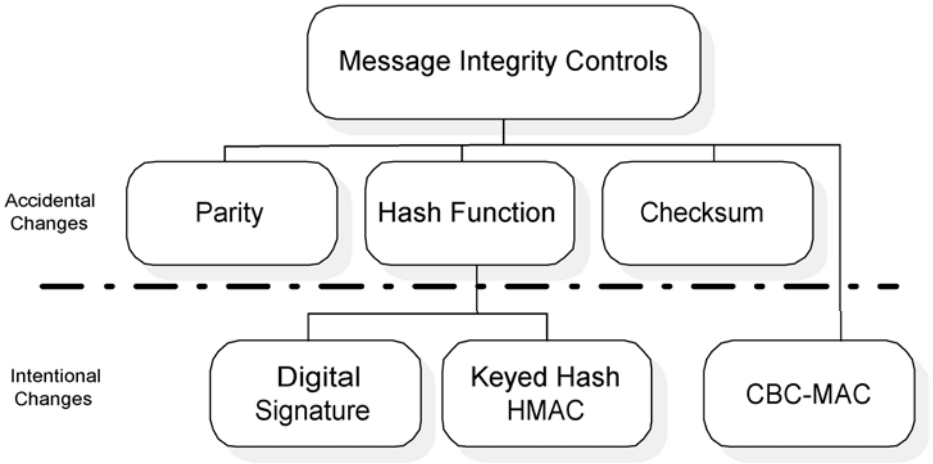
Domain Agenda

- Introduction
- Cryptography
  - Introduction to Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - **Message Integrity Controls**
  - Key Management
  - Uses of Cryptography
  - Legal Issues
- Cryptanalysis
- Information Hiding Techniques

Message Integrity Controls

- Allows for the detection of alterations
- Special values are added to the message
- Special branch of cryptography has been developed to create one-way functions

Message Integrity Controls



Hash Functions

- List of Hash Algorithms
  - Division-remainder Method
  - Folding
  - Radix Transformation
  - Digit Rearrangement
- Advantages of Cryptographic Hash Algorithms
  - Reduce collision
  - Increase sensitivity to changes

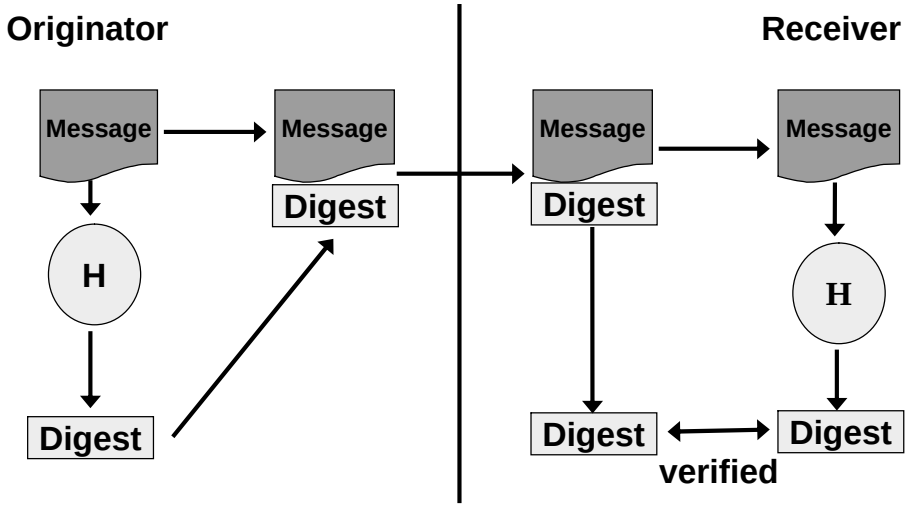
Hash Functions Characteristics

- Result in a 'condensed representation' of the original message
- Should be a one-way function
- Non-linear relationship between hashes
- Should resist birthday attacks
- Should derive the hash using the whole, original message

Common Hash Functions

- MD2/MD4/MD5
- Secure Hash Algorithm (SHA)

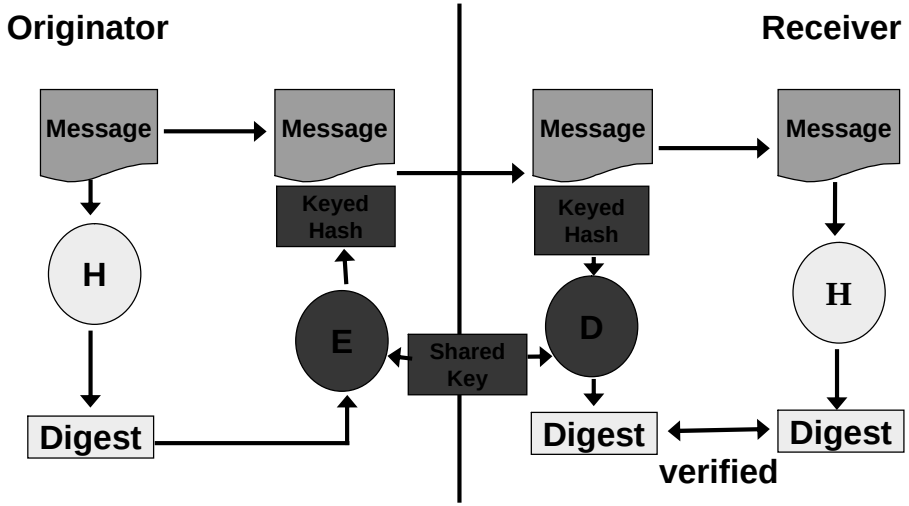
Operation of Hash Functions



Keyed Hashes

- Intended to provide greater ability to prove that message has not been altered
- Combines non-keyed hash function with symmetric key cryptography
- Examples
  - Key-Hashed Message Authentication Code (HMAC)
  - CBC-MAC

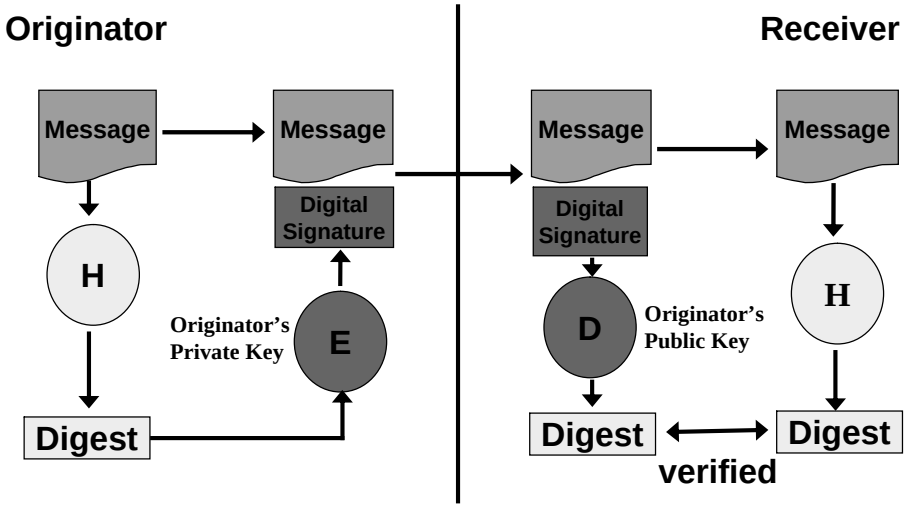
Operation of Keyed Hashes (HMAC)



Digital Signatures

- Provides sender authenticity checking and non-repudiation using asymmetric key cryptography
- Sender's private key is used to "encrypt" the hash
- Recipient uses sender's public key to check the signature and verifies the hash

Operation of Digital Signatures



Domain Agenda

- Introduction
- Cryptography
  - Introduction to Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Message Integrity Controls
  - **Key Management**
  - Uses of Cryptography
  - Legal Issues
- Cryptanalysis
- Information Hiding Techniques

Functions of Key Management

- Key Creation and Derivation
- Key Distribution and Update
- Verification of Trustworthiness of Keys
- Proper Storage and Destruction of Keys
  - Trusted Hardware
- Recovery or Revocation of Lost Keys
  - Key Escrow and Multi-party Control of Keys
- Determination of Appropriate Key Sizes
  - Based on required strength

Key Derivation Functions (KDFs)

- Cryptographic hash functions that use a secret or known value to generate symmetric keys
- Combines three different values to generate keys
- Iterations - The number of times the function will be run to generate keys

Key Agreement Schemes

- Diffie-Hellman
- Unified Diffie-Hellman
- MQV (Menezes-Qu-Vanstone)

Diffie-Hellman Key Agreement Operation

Step	Alice	Exchange Methodology	Bob
1	Select Y & P with Bob	$Y^X \pmod P$ Publicly known to the world	Select Y & P with Alice
2	Y = 11 P = 13	$11^x \pmod{13}$	Y = 11 P = 13
3	Alice chooses a secret number (2)	Select a secret number	Bob chooses a secret number (5)
4	$11^2 \pmod{13}$ 121 (mod 13) = 4	Calculate one-way function using their secret number	$11^5 \pmod{13}$ 161,051 (mod 13) = 7

Diffie-Hellman Key Agreement Operation

Step	Alice	Exchange Methodology	Bob
5	Alice sends the result "4" to Bob	Send the result of the one-way function to the other person	Bob sends the result "7" to Alice
6	Calculate $7^2 \pmod{13}$ 49 (mod 13) = 10	Take received calculation and raise it to your secret number	Calculate $4^5 \pmod{13}$ 1024 (mod 13) = 10
7	Symmetric key selected through calculation is 10	Both people have the same number without revealing their "secret"	Symmetric key selected through calculation is 10

Trust and Trust Models

- Trustworthiness of keys can be difficult
- Two main trust models
- Certification establishes trustworthiness

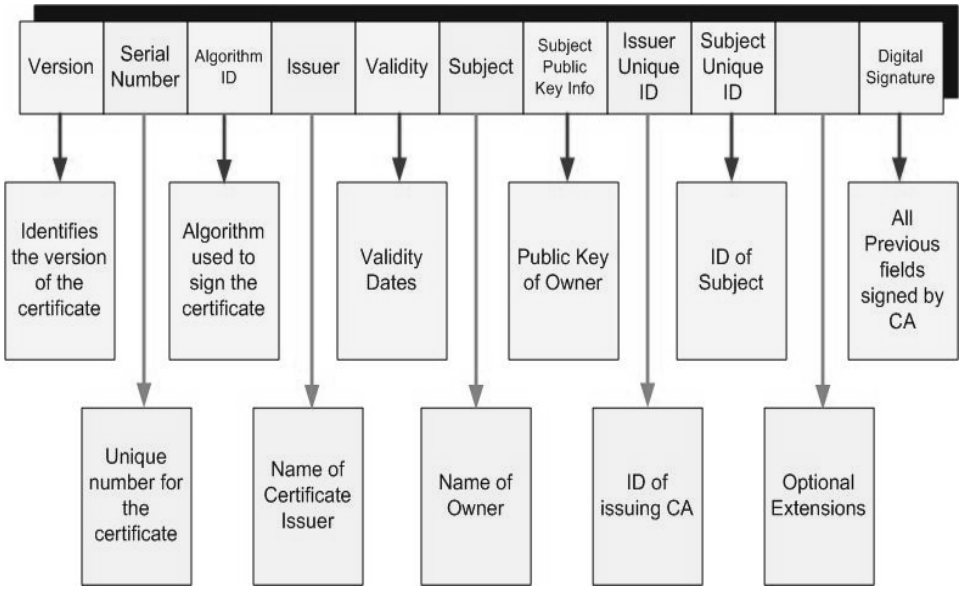
Public Key Infrastructure

- Binds a person/entity to their public keys
  - Binding is done through certification
- Certified public keys are published as digital certificates
- Cross-Certification

Certification Authority

- Manages certificate
- Acts as a trusted third party
- Offer various classes of digital certificates

Contents of an X509v3 Digital Certificate



Domain Agenda

- Introduction
- Cryptography
  - Introduction to Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Message Integrity Controls
  - Key Management
  - **Uses of Cryptography**
  - Legal Issues
- Cryptanalysis
- Information Hiding Techniques

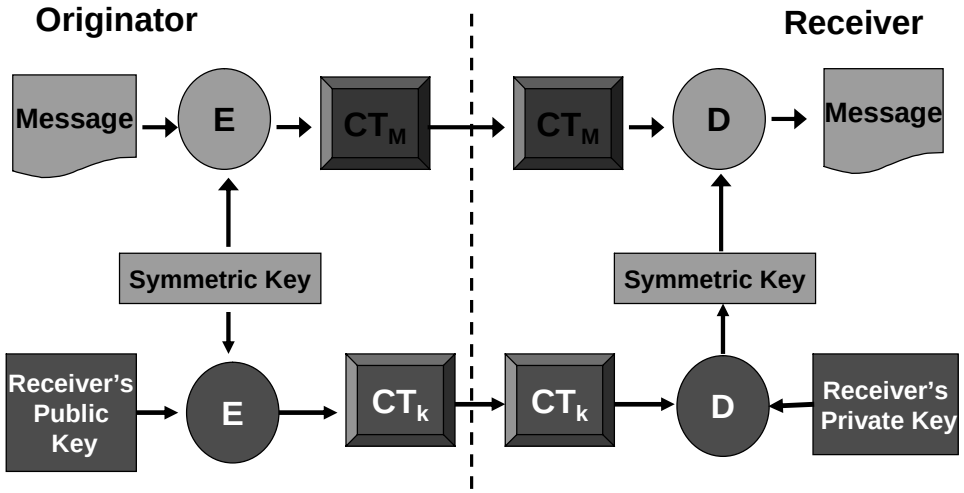
Uses of Cryptosystems

- Common Goals
- Used for secure
  - Data Storage
  - Email
  - Network Protocols

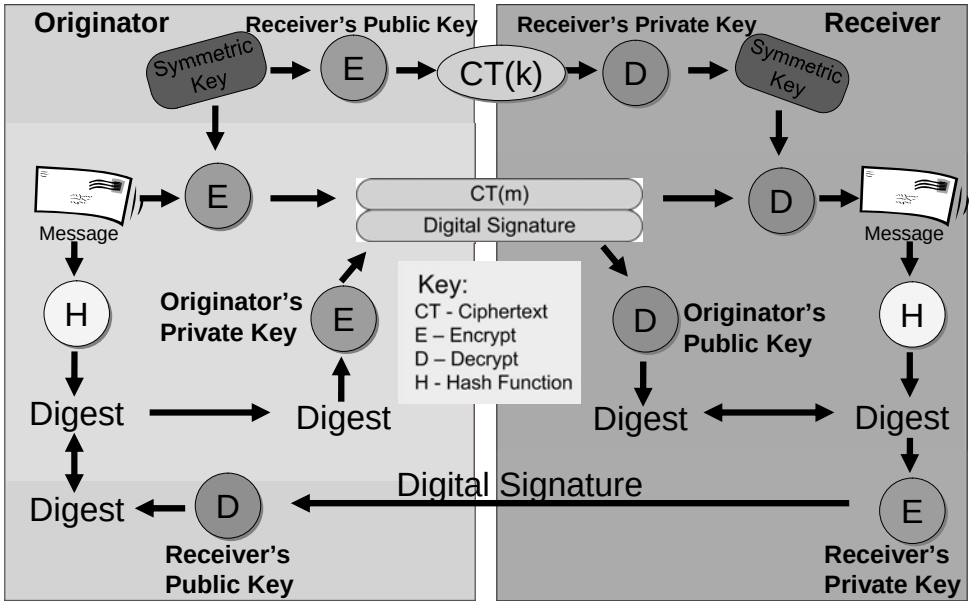
Hybrid Systems

- Maximizes strengths
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Message Integrity Controls

Simple Hybrid System Operation



Example of a Complex Hybrid System



Common Secure Email Protocols

- Message Security Protocol (MSP)
- Privacy Enhanced Mail (PEM)
- MIME Object Security Services (MOSS)
- Pretty Good Privacy (PGP)
- Secure Multipurpose Internet Mail Extensions (S/MIME)

Secure Network Protocols

- Examples of Secure Network Protocols and Implementations
  - Secure HTTP (S-HTTP)
  - Secure Shell (SSH)
  - Secure Socket Layer (SSL)
  - Transport Layer Security (TLS)
  - IPSec
  - WiFi Protected Access (WPA)
  - 802.11i Wireless LAN (WPA2)

Domain Agenda

- Introduction
- Cryptography
  - Introduction to Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Message Integrity Controls
  - Key Management
  - Uses of Cryptography
  - **Legal Issues**
- Cryptanalysis
- Information Hiding Techniques

National Policies and Controls

- Controls can be put into three rough categories
  - Export Controls
  - Import Controls
  - Domestic-Use Controls
- National policies are extremely varied

International Policies and Controls

- Wassenaar Arrangement
- Council of Europe Convention on Cybercrime (2001)
- European Union

Domain Agenda

- Introduction
- Cryptography
  - Introduction to Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Message Integrity Controls
  - Key Management
  - Uses of Cryptography
  - Legal Issues
- **Cryptanalysis**
- Information Hiding Techniques

Strength of Algorithms and Cryptosystems

- Dependent on a number of factors
  - Key Space
    - Related to bit-size of the key
  - Algebraic strength of the algorithm itself
  - Correct Implementation

Common Weaknesses

- Insufficient Key Space
- Poor Key Management
  - Malleability
  - Poor Diffusion or Confusion
  - Poor Random Number Generation
- Key Clustering

Selection of a Strong Cryptographic Solution

- Use evaluated solutions
- High Work Factor
- Publicly-evaluated Cryptographic Algorithms

Cryptanalysis

- Art and Science of Breaking Codes
- Techniques
  - Attacking the Key
  - Attacking the Algorithm
  - Attacking the Implementation
  - Attacking the Data (ciphertext or plaintext)
  - Attacking the People - Social Engineering

Common Cryptanalytic Techniques

- Brute-force Attack
- Plaintext Attacks
- Ciphertext Attacks
- Man-in-the-Middle Attack
- Meet-in-the-Middle Attack and other Analytic Attacks
- Side Channel Attacks

Brute Force Attack

- Trying all possible combinations
- Two factors: Cost and Time
  - Moore's Law
  - Measured in MIPS per year

Time of Brute Force

Bits	Number of keys	Brute Force Attack Time
56	7.2×10^{16}	20 hours
80	1.2×10^{24}	54,800 years
128	3.4×10^{38}	1.5×10^{19} years
256	1.15×10^{77}	5.2×10^{57} years

Attacks

- Plaintext
  - Known-Plaintext Attack
  - Chosen Plaintext Attacks
  - Adaptive Chosen Plaintext Attacks
- Ciphertext
  - Ciphertext-Only Attack
  - Chosen Ciphertext Attack
  - Adaptive Chosen Ciphertext Attack

Other Common Attacks

- Meet-in-the-Middle Attacks and other Analysis Attacks
- Slide Attacks
- Man-in-the-Middle Attacks
- Side Channel Attacks (Timing and Power Attacks)

Attacks Against Ciphers

- Stream
  - Frequency Analysis and other Statistical Attacks
  - IV or Keystream Analysis
- Block
  - Linear Cryptanalysis
  - Differential Cryptanalysis
  - Linear-Differential Cryptanalysis
  - Algebraic Attacks
  - Frequency Analysis

Attacks Against Hash Functions

- Dictionary Attacks
- Birthday Attacks

Non-Technical Attacks

- Social Engineering
  - Persuasion
  - Coercion (Rubber-Hose Cryptanalysis)
  - Bribery (Purchase-Key Attack)
- Theft

Domain Agenda

- Introduction
- Cryptography
  - Introduction to Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Message Integrity Controls
  - Key Management
  - Uses of Cryptography
  - Legal Issues
- Cryptanalysis
- **Information Hiding Techniques**

Steganography

- Art of hiding information
- Plaintext hidden/disguised
- Prevent a third party from knowing that a secret message exists
- Traditionally accomplished in a number of ways
  - Physical Techniques
  - Null Ciphers

Modern Steganography

- Extends traditional techniques
  - Use of least significant bits
  - A slight change to the values does not have a visible effect on the contents

Modern Steganography

- RGB values have been altered to contain a secret message

E1089197693F6C4C26E0033F8C8AF00C

57694B77DCB55C543C6C0BA8E1FF2D17

- File sizes are identical, change can be detected through the use of a common Message Integrity Control (MD5)

Digital Watermarking/Rights Management

- Digital Watermarking
- Digital Rights Management (DRM)

Domain Summary

- Cryptographic Concepts and Algorithms
- Message Integrity Codes
- Digital Signatures and Certification
- Cryptanalysis