INFO 6010 Lesson 5
Security Architecture and Engineering Part 2
Domain 3
Cryptography

Revision 2

Information Security Management & Network Security Architecture

FANSHAWE

Discussion Items

- Security Architecture & Engineering - Cryptography
- History of cryptography
- Cryptography components and their relationships
- Government involvement in cryptography
- Symmetric and asymmetric key algorithms
- Public key infrastructure (PKI) concepts and mechanisms
- Hashing algorithms and uses
- Types of attacks on cryptography

Cryptography

- Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process.
- The science of protecting information by encoding information into unreadable format.
- Effective way of protecting sensitive information as it is stored or transmitted

Goal of Cryptography

- Hide information from unauthorized individuals
- First encryption dates back 2000 B.C.
- Encryption used as a tool in warfare, commerce and governments
- Encryption algorithms and devices that use them have increased in complexity
- Changes in cryptography closely follow advances in technology

Cryptography

- Cipher is another term for algorithm
- Monoalphabetic and Polyalphabetic ciphers are examples of a *substitution* cipher
- Monoalphabetic cipher
  - Means one alphabet is used
- Polyalphebtic
  - more than one alphabet

History of Cryptography

- ATBASH encryption scheme:
  - Hebrew cryptographic cipher
- Simple form of substitution for encryption
  - Each letter in the alphabet was mapped to a different letter in the alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

YXVUTSRQPONMLKJIHGFEDC

History of Cipher

- Around 400 B.C. the Spartans used a system where they would wrap a piece of papyrus around a staff or wooden stick. Both parties had to have same size stick for letters to line up properly. This was called a Scytale Cipher method

Caesar Cipher

- 100-44 B.C. Julius Caesar developed a simple method by shifting letters of the alphabet, similar to atbash scheme.
- Letters shifted by three positions.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

ROT 13

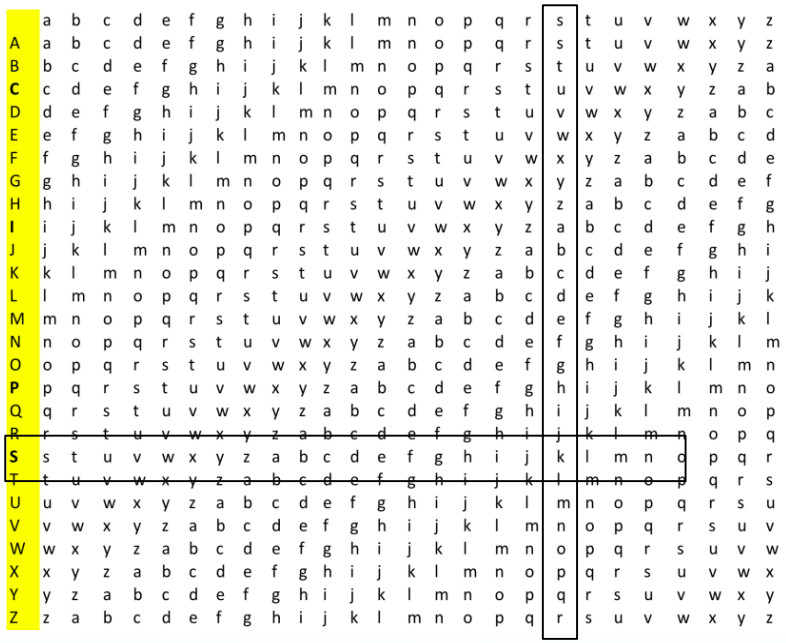
- A more recent encryption method
  - Not very sophisticated
- Used in the 80's mainly online forums (BBS)
- Not used to protect data but to hide (obscure) text by requiring simple decryption
- Used Caesars method, shifted letters 13 spaces

ABCDEFGHIJKLMNOPQRSTUVWXYZ

NOPQRSTUVWXYZABCDEFGHIJKLM

Vigenere Cipher

- 16th century France
- Blaise de Vaginere designed a *polyalphabetic* cipher for Henry III
  - Uses 27 shift alphabets with letters shifted one position

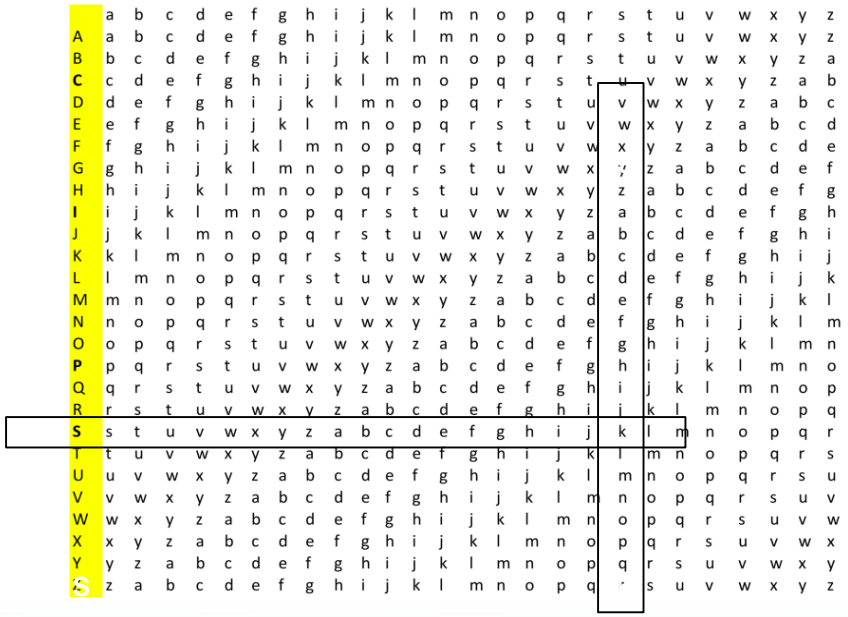


	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	u
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	u	v
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	u	v	w
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	u	v	w	x
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	u	v	w	x	y
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	u	v	w	x	y	z

The intersection of the rows and columns determine the cipher text based on a secret key

Vigenere Cipher

- Example from textbook pg. 344
  - Secret key *security*
  - Plain text system
  - Follow 1st letter of key along top row to S column
  - Follow 1st letter of plain text to row S

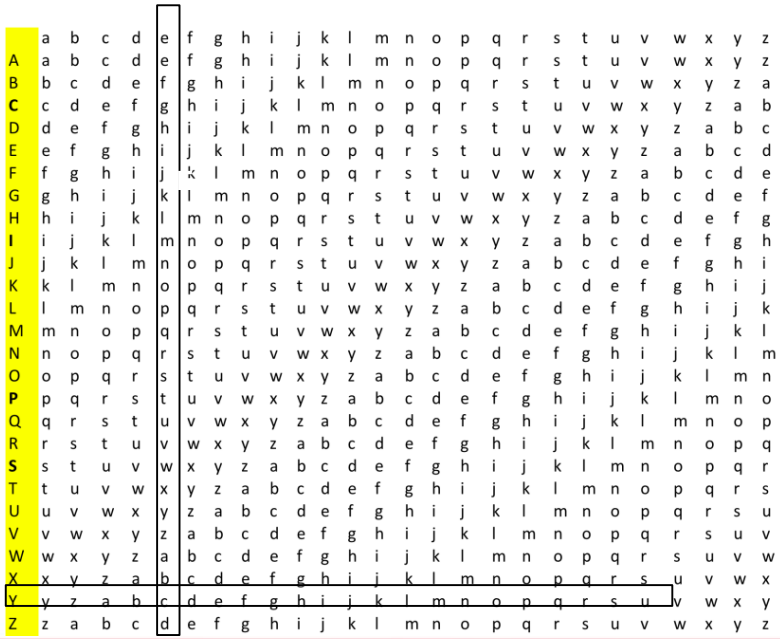


Intersect at letter **K**

1st letter of cipher text

Vigenere Cipher

- 2nd letter of cipher text
  - 2nd letter of key is e (secret key *security)*
  - 2nd letter of plain text word *system*
  - Follow 2nd letter of key along top row to E column
  - Follow 2nd letter of plain text to row y



Intersect at letter **C**

2nd letter of cipher text

1st two letters of cipher text become kc

Enigma

- Used by the Germans during World War II
- Electro-mechanical rotor machine
  - Mechanical method of determining cipher text
  - Letter typed in keyboard produces a corresponding letter in cipher text
- Polish cryptographer broke Germany's Enigma ciphers 5 weeks before the start of World War II.
- Gave French and British tactical advantage as most German messages could be deciphered

Enigma

- The mechanical parts act in such a way as to form an electrical circuit
- When a key is pressed, the circuit is completed and ultimately lights one of the display lamps indicate the output letter.

Cryptography

- Invention of computers has expanded encryption methods exponentially
- Cryptographic designers could develop new and very complex ciphers
- IBM worked on a project called ‘Lucifer’
  - Introduced mathematical equations and functions
  - 1976 National Security Agency (NSA) established (DES) Data Encryption Standard

Cryptanalysis

- Cryptography is now used to protect data, financial transactions, corporate transmissions, email messages, web transactions, wireless communication, storage of confidential information
- Gives rise to Cryptanalysis
  - Science of studying and breaking the secrecy of encryption processes
  - Reverse engineer algorithms and keys
  - Compromise authentication schemes

Encryption

- Encryption is a method of transforming readable data, called plaintext into a form that appears to be random and unreadable, which is called cipher text
  - Plaintext is readable by human and machine
  - Cipher text is not readable by human or computer
- Enables transmission of confidential information over insecure channel

Encryption

- Data when stored on a computer can be protected by various access controls
  - Physical and logical
- Data that is transmitted over wire or wireless cannot take these controls for granted
  - Much more vulnerable

Cryptosystem

- Any system or product that provides encryption and decryption service
  - Cryptosystem can be software or hardware
- Cryptosystem uses an encryption algorithm
  - Determines complexity of encryption
- Cryptosystem uses keys
  - Secret value which works with the algorithm to encrypt and decrypt

Cryptosystem

- Algorithm also known as cipher is a set of rules dictating how enciphering and deciphering takes place.
- Many of today's mathematical algorithms are publicly known and are not the secret part of the encryption process
- A cryptosystem includes the following components:
  - Software
  - Protocols
  - Algorithms
  - Keys

Encryption Key

- The key is the what makes encryption secret and confidential
- The key also known as the crypto variable is a value that comprises a large sequence of random bits.
- A key is generated from something called a keyspace
  - Keyspace is a range of values which can be used to generate a key
- The larger the keyspace the more random the keys, and harder to break

Encryption Key

- Large keyspace allows for more possible keys
- Today we commonly use 128bit, 512bit or 1024bit keys
- Encryption algorithms should use entire keyspace when generating a key
- Key should be as random as possible within the defined keyspace

Kerckhoff's Principle

- Encryption vs. Secrecy
- Auguste Kerckhoffs paper published in 1883
- A cryptosystem should be secure even if everything about the system, except the key is public knowledge.

Kerckhoff's Principle

- Stated that the only secrecy involved with cryptography system should be the key
  - A hackers knowledge of the mathematics of the algorithm will not allow them to decipher the message with out the key
- Argued the algorithm itself should be publicly known
- If security based on too many secrets there would be more vulnerabilities

Kerckhoff's Principle

- Public Knowledge vs. Secrecy
- Public Knowledge
  - Weaknesses and flaws easier to find and fix
  - More eyeballs looking at algorithm
- Secrecy
  - Smaller number of people make algorithm more secure

Cryptography

- Work Factor
  - Time and how many resources and how long an attacker would require to break key
- Protect your key.
  - Otherwise the strongest algorithm and key become useless if you give it away

Cryptosystem Services

- Confidentiality
  - Ensure only authorized can decrypt
- Integrity
  - Ensure message is not altered
- Authentication
  - Verify identity of user or system
- Authorization
  - Upon proving identity the user is granted key that will allow access
- Nonrepudiation
  - Ensures sender cannot deny sending

One Time Pad

- Invented by Gilbert Viernam in 1917
- Considered unbreakable if implemented properly
  - Does not use alphabet shift, Caesar or Vigenere ciphers
- Uses a PAD made up of random values
- Uses exclusive OR (XOR) technique
- When comparing values if both values are the same the result is ‘0’
  - (0 XOR 1 =1)
  - (1 XOR 0 =1)
  - (1 XOR 1 = 0)

One Time Pad

- Plain text message must be converted to into bits of 1 and 0
- Pad is also made up of bits (1's and 0's)
- Message Stream: 1 0 0 1 0 1 0 1 1 1
- Keystream (PAD): 0 0 1 1 1 0 1 0 1 0
- Ciphertext Stream: **1 0 1 0 1 1 1 1 0 1**

Cryptography

- XOR encryption is considered unbreakable if the following are true:
  - Pad (key) is same length as message
  - Pad (key) is only used once
    - Patterns may appear allowing breaking
  - Pad (key) is securely distributed
  - Pad (key) is made of truly random numbers
- Problems with XOR Technique
  - Pad (key) management becomes a nightmare
  - Impractical in most situations

Running Key Cipher

- Use components of physical world
- Use a book then specify page numbers, line numbers and words
- Reader and sender agree to use a specific book to conceal their message
- Cipher could be a book page, line number and column count

Running Key Cipher

- Message from the sender:
  - 135l7c5.289l5c5.312l8c1
- This could mean:
  - 1st book in predetermined list
  - 35th page
  - Line 7
  - Column 5

Running Key Cipher

- Write down letter found in that location
  - 2nd book in predetermined list
  - 89th page
  - Line 5
  - Column 5
- Write down letter found in that location

Concealment Cipher

- Message within a message
- Sender and recipient have agreed every 2nd word is our key value
- Cipher text
  - The Fanshawe student is bringing cold back today
  - If we chose every 2nd word clear text message is;
  - Fanshawe is cold today

Steganography

- Hiding data in another media type so the existence of data is concealed
- Example of Steganography:
  - Hiding messages in graphic images
- Can be hidden in other media
  - Wave file
  - Document file
  - Other type of media

Steganography

- Message is not encrypted, just hidden
  - Security through obscurity
  - Many tools do offer encryption as an option
- Media files are ideal for Steganography because of large file sizes
- Example
  - Every 100th pixel could correspond to a letter in the alphabet
  - Least significant bit of a pixel is replaced with bit of hidden message
  - Change in colour of pixel can not be detected by human eye

Steganography

- Carrier
  - A signal, data stream or file that has hidden information (payload) inside of it
- Stego-medium
  - The medium used to transfer the hidden information
  - Disk, web site, email
- Payload
  - The information that is to be concealed and transmitted

Steganography

- Many types of file have some bits that can be modified and not affect the file they are in
- This is where secret data can be hidden without altering the file in a visible manner
- (DRM) Digital Rights Management and Digital Watermark are examples of Steganography
- Deter users from copying material

Types of Ciphers

FANSHAWE

Cipher

- Substitution Cipher - replaces bits, characters or blocks or characters with different bits characters or blocks
- Transposition Cipher - does not replace text but rather moves the original values around
  - The values are scrambled or put in different order
- Both a methods used by symmetric encryption ciphers

Cipher

- Substitution ciphers use a key to dictate how the substitution should occur
- Caesar cipher replaced every letter with one three placed beyond it
- Caesar is a very simple example of how it works
- Today substitution ciphers are very complex

Transposition Cipher

- Mathematical functions and formulas used by transposition ciphers are very sophisticated and difficult to break
- The algorithm contains the possible ways that substitution and transposition process can take place
- The key is used as instructions for the algorithm dictating how and in what order these processes will occur

Cipher

- Simple implementations of substitution and transposition ciphers are vulnerable to attacks that perform frequency analysis
- In most languages certain letters appear more often in English it is E
- Analyst may look for pattern most frequent in message and substitute letter E to gain foothold.
- Substitution and transposition methods use complex mathematics to avoid frequency analysis

Cryptography

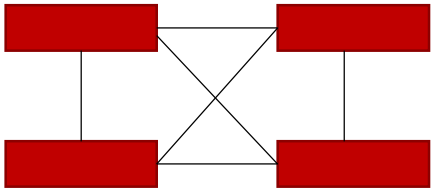
- Two main parts to encryption are the algorithm used and the key
- Algorithms have the mathematical formulas that dictate the rules how plaintext will be turned to cipher text
- Keys are random bits that will be used by the algorithm to specify how the plain text is converted
  - Randomness of the encryption process
- For a sender to share a message with recipient privately both must have the same algorithm and private key

Symmetric Encryption

- Sender and receiver use the same key for encryption and decryption
- If sender and receiver wish to communicate they must have two instances of same key
- Keys must remain secret by each party
- Provides confidentiality

Symmetric Encryption

- If 10 people wanted to communicate secretly with each other 45 keys are required
- Formula to calculate number of symmetric keys required
- N(N-1)/2 = number of keys
  - 2 people 2(2-1)/2=1
  - 3 people 3(3-1)/2=3
  - 4 people 4(4-1)/2=6



With 4 people
6 different conversations
Require 6 secret keys

Symmetric Encryption

- Strength
  - Faster then asymmetric
  - Hard to break if using a large key size
- Weakness
  - Requires a secure mechanism to deliver keys
  - Each pair of users require a unique key
  - More pairs more keys
  - Managing secret exchange of keys is difficult
- Examples of symmetric encryption algorithms
  - DES, 3DES, Blowfish, RC4-6, AES

Asymmetric Encryption

- Sender and receiver use different keys that are mathematically related
- Message encrypted with one key and decrypted with the other key
- Not possible to encrypt and decrypt with same key
- Key pair is made up of public and private keys
- Public key can be known to everyone
- Private key must be kept secret and used only by the owner
- Impossible to calculate private key from public key

Asymmetric Encryption

- Decrypting a message using the public key provides authentication
  - Because the sender with the related private key and is the only one that could have encrypted the message
- If a message is encrypted with a public key it provides message confidentiality
  - Only the recipient with the related private key can decrypt the message
  - Another public key can not decrypt the message

Asymmetric Encryption

- Open message format
  - Encrypting a message with senders private key.
  - Does not give confidentiality because anyone with public key can decipher message.
- Secure message format.
  - If confidentiality is required receiver can reply to message and encrypt using senders public key
  - Can only be decrypted with related private key
  - But this does not provide authentication because anyone may have access to public key.

Asymmetric Encryption

- Strength
  - Better key distribution systems developed than symmetric
  - Can provide authentication and nonrepudiation
- Weakness
  - Much slower than symmetric
  - Mathematically intensive task
- Examples
  - RSA, Diffie-Hellman, ECC, DSA, El Gamal , Knapsack

Symmetric Algorithms

- Symmetric algorithms have two main types
- Block Ciphers – work on blocks of bits
- Stream Ciphers – work on bits one byte at a time

Block Cipher

- Message divided into blocks of bits.
- Message put through the mathematical functions one block at a time
- 32, 64 and 128 bit blocks used by algorithms

Block Cipher

- For a cipher to be considered strong it must contain two attributes:
- Confusion
  - Carried out through substitution
- Diffusion
  - Carried out through transportation
- An algorithm will have many rounds of substitution and transposition
- If cipher has both attributes reverse engineering is impossible

Stream Cipher

- Symmetric Algorithm
- Performs mathematical computation on each bit one at a time in a stream of bytes
- Stream ciphers use keystream generators
  - Key is a stream of bits that is XORed with the plaintext bits to produce cipher text
- Key provides randomness of the encryption process
- The sender and receiver must have the same key to generate the same keystream

Stream Cipher

- A strong and effective stream cipher contains the following characteristics;
  - Long periods of no repeating patterns within keystream values
  - Statistically unpredictable keystream
  - A keystream not linearly related to key
  - Statistically unbiased keystream (as many 0's and 1's)
- Stream ciphers require a lot of randomness.
- Requires more processing power then block ciphers

Initialization Vectors

- Random values that are used with algorithms to ensure patterns are not created during the encryption process
- They are used with keys and do not need to be encrypted when sent to destination
- If IV's are not used then two identical plaintext values that are encrypted with the same key will create the same cipher text
- Providing such patterns to attackers can aid in breaking encryption
- Key and IVs are used to generate more randomness

Hybrid Systems

- Asymmetric and symmetric algorithms used together
- Public key cryptography used for protecting the secret key symmetric algorithm used for bulk encryption.
- Symmetric key is used to encrypt actual message data
- Asymmetric public key is used to encrypt the symmetric key for secure key exchange between sender and receiver

Session Key

- Symmetric key used to encrypt messages between two users.
- It is generated at start and destroyed once a session has been completed.
- More secure because each communication uses a new key.
  - Temporary key

Symmetric Keys

- Common symmetric key terms
- Single key cryptography (one key)
- Secret key cryptography (static key)
- Session key cryptography (dynamic key)
- Private key cryptography (only one key used)

Types of Symmetric systems

FANSHAWE

DES

- DES - Data Encryption Standard
  - Standard from NIST
    - National Institute of Standards and Technology
  - Digital Encryption Algorithm - DEA
  - Symmetric block algorithm using 64bit key
  - 56bit key and 8 bits for parity
  - 16 rounds of transposition and substitution functions
  - The order and type of transposition and substitution varies with key value

Based on IBM Lucifer 128 bit key algorithm

DES

- 56 bit DES key broken in 1998
- 3 days with brute force attack
- 1536 40MHz processors
- 60 million decryptions per second
- 56 bit key has 72 quadrillion possible key values
  - Computer system developed by Electronic Frontier Foundation
  - Called DES Cracker or Deep Crack

DES Modes

- DES and other block ciphers have different modes of operation that may be better suited for a situation
- EBC – Electronic Code book
- CBC – Cipher Block Chaining
- CFB – Cipher Feedback
- OFB – Output Feedback
- CTR – Counter Mode

EBC Mode

- The key becomes the code book (instruction) for how substations and permutations performed
  - Easiest & fastest method
- Each 64 it block uses same key
- Not a high degree of randomness compared to other methods
- Each plain text block gives the same cipher text

EBC Mode

- Best suited for small amounts of data such as PINs or challenge-response messages
- Good for database because each record is an independent block
  - Fast to decrypt individual records from large database without decrypting the complete database

CBC Mode

- With CBC the previous block is used as input into next plain text block
- The cipher text result will always be different for the same 64 bit block of plain text
  - Ist block is encrypted with key
  - The resulting cipher text is XORed with next plain text block
  - This XOR result is then encrypted with the key to get the next block of cipher text
  - Each block modifies the next block before encryption
  - A 64 bit IV is used to XOR with the first block to start the chain
- Best used for large blocks of data

CFB Mode

- Combination of block and stream cipher
- Encrypts data one byte at a time
- Best for encrypting keystrokes and mouse movements across a network to a backend terminal server
- Key and IV create a keystream
- The encrypted byte is transmitted across network
- Encrypted byte is used as input into next plain text byte before encryption with key stream

OFB Mode

- Used like CFB when small amounts of data need to be encrypted
- Input into next plain text comes from keystream not from the resulting cipher text

- CFB has chance that a corrupted bit will corrupt the cipher text output which cascades through each block
- More reliable

CTR Mode

- An IV is used as input with key to create the cipher text
- IV is not random for each block but increased by a counter
- No chaining of a cipher text block into next plain text encryption
- Blocks can be encrypted in parallel for faster operation
- Used in IPSec, IEEE802.11i
- Packets sent over a network may nor arrive in order
- Decryption can start on a block without waiting for previous blocks of cipher text in a chain

3DES

- Quick fix to DES problem
- Uses 48 rounds of transposition and substitution functions
- 3 times longer to encrypt and decrypt. more horsepower
- As open standard available as an option in most cryptosystems

3DES Modes

- DES – EEE3
  - 3 encryption keys and 3 steps encrypt-encrypt-encrypt
- DES- EDE3
  - 3 encryption keys and 3 steps encrypt-decrypt-encrypt
  - Decryption step with a different key further scrambles message
- DES – EEE2
  - 2 encryption keys and 3 steps encrypt-encrypt-encrypt
  - 1st and 3rd encryption steps use same key
- DES – EDE2
  - 2 encryption keys and 3 steps encrypt-decrypt-encrypt
  - 1st and 3rd encryption steps use same key

AES

- AES - Advanced Encryption Standard
  - Based on Rijndael cipher
  - Replacement for DES
- 128 bit symmetric block cipher
- Key sizes 128,192 and 256 bits
- The number of operations and rounds of encryption depend on key size
- Original Rijndael cipher allowed for variable block sizes

AES

- Execution steps based on key size
  - 128 bits = 10 rounds
  - 192 bits = 12 rounds
  - 256 bits = 14 rounds
- Low memory usage

IDEA

- IDEA - International Data Encryption Algorithm
- 64 bit block cipher with 128 bit key
  - Divided into 16 smaller blocks with 8 rounds of computation against each block
  - Faster than DES
  - Harder to break then DES because longer key
  - Used in PGP
- Patent held so licensing required

Blowfish

- 64 bit Block cipher
- Key can be 32 bit to 448 bit
- 16 rounds
- Public domain cipher and can be freely used
  - Bruce Schneier

Rivest Ciphers

- RC4
  - Stream cipher with variable key length
  - Used in SSL and WEP
  - Simple, fast and efficient
- RC5
  - 32, 64 or 128 bit block cipher
  - Variable key size to 2048 bits
  - Variable number of encryption rounds up to 255
- RC6
  - Block cipher built upon RC5 to improve performance

Cryptography

- Symmetric key cryptography has the following drawbacks
- Security Services
  - Used just for confidentiality
  - Not suitable for authentication or nonrepudiation
- Scalability
  - Number of keys increase with number of users
- Secure key distribution
  - How to ensure key delivered to other end without being exposed

Diffie-Hellman

- First asymmetric algorithm
- Developed to address problem of secure distribution of symmetric secret keys
- Martin Hellman & Whitfield Diffie
- Algorithm computes keys based on discrete logarithms in a finite field

Diffie-Hellman

- Both hosts send each other their public keys
- Both hosts complete the Diffie-Hellman algorithm calculation with their private keys and the received public key
- Both ends will calculate the same value
- This becomes symmetric key
- Vulnerable to man in the middle attack as it does not use authentication prior to sending public keys

RSA

- De facto industry standard
- Used for the following purposes
  - Encryption
  - Digital signatures
  - Key exchange
- Security comes from the difficulty of factoring large numbers
- Public & private keys are a function of 2 large prime numbers

El Gamal

- El Gamal
  - Public key algorithm that can be used for
  - Digital signatures
  - Encryption
  - Key exchange
- Based on calculating discrete logarithms in a finite field.
  - Extension of Diffie-Hellman
  - Main drawback is performance.

Elliptic Curve Cryptosystem

- ECC
- Most efficient asymmetric algorithm
- Algorithm based on computing discrete logarithms on elliptic curves
  - Pubic and private keys are points on curve
- Offers same security but with smaller key size

Hash Algorithms

- One way function that takes a variable length string (message) and produces a fixed length value.
- Used to verify integrity of message
  - Can not be reversed to find original message
- Receiver must run message through the same hash algorithm to compare hash values
- Vulnerable to man in the middle
  - No secret keys used
- Need message authentication code to further secure message

Hash Process

1. The sender puts the message through a hashing function
2. A message digest value is generated
3. The message digest is appended to the message
4. The sender sends the message to the receiver
5. The receiver puts the message through a hashing function
6. The receiver generates her own message digest value
7. The receiver compares the two message digest values. If they are the same the message has not been altered

HMAC

- Hashed Message Authentication Code
- Similar to hash but adds a MAC value
  - Message Authentication Code
- A secret value (key) is concatenated with message.
- Result is put thought hashing algorithm
- A HMAC value is generated
- HMAC value is appended to message.
- Both parties need same secret value to compute hash

HMAC Process

1. The sender concatenates a secret key with the message
2. The result is put through a hashing algorithm
3. A MAC value is generated
4. The MAC value is appended to the message
5. The sender sends the message with the attached MAC value to the receiver
   - The sender does not send the secret key with the message
6. The receiver concatenates the secret key with the message
7. The receiver puts the results through a hashing algorithm and generates a MAC value
8. The receiver compares the two MAC values. If they are the same, the message has not been modified

CBC-MAC

- The original message is encrypted with a CBC *(Cipher Block Chaining – Message Authentication Code)* symmetric algorithm
- The cipher text is hashed
- The hash is sent along with plain text message
- Receiver encrypts message and creates a hash
- If hash values are same message has not been altered
- Depends on symmetric key value at each end

Hash Algorithms

- Purpose of one way hash function is to provide a fingerprint of the message
- A hash function should not provide the same hash value for two or more different messages
- If this is true it is called “collision free”
- Good cryptographic hash functions should have the following characteristics:
  - The hash should be computed over the entire message
  - The hash should be a one-way function so messages are not disclosed by their values
  - Given a message and its hash value, computing another message that has the same has value should be impossible
  - The function should be resistant to birthday attacks

Hash Algorithms

- MD2
  - One way hash designed by Ron Rivest that creates 128 bit message digest value
  - Not weaker then any other MD family but lacks performance
- MD4
  - One way hash function designed by Ron Rivest that creates 128 bit message digest value
  - High speed performance for software implementation

Hash Algorithms

- MD5
  - One way hash function designed by Ron Rivest that creates 128 bit message digest
  - Improved version of MD4
  - MD5 added a fourth round of operations during the hashing mechanism to provide higher level of security
  - Has been shown to be subject to “collision” attacks
  - No longer recommended for SSL certificates and digital signatures

Hash Algorithms

- SHA-1
  - Strong Hash Algorithm
  - Designed by NSA for NIST
  - Used for Digital Signature Standard
  - 160 bit hash
  - Based on MD4 algorithm
- SHA-1 family
  - Longer hash outputs
  - SHA-256 256 bit hash
  - SHA-512 512 bit hash
  - SHA-2 and 3 families considered secure for all uses.

Hash Attacks

- Attacks against one-way hash functions
- A good hashing algorithm should not produce the same hash value for two different messages
  - If it does this is called a collision
- Birthday Attack
  - Attacker attempts to force a collision
  - Based on the mathematical birthday paradox that exists in standard statistics
  - That 2 people in a group will have same birthday
  - In a group of 23 two will have same birthday

Public Key Infrastructure - PKI

FANSHAWE

PKI

- Public key infrastructure (PKI)
  - Consists of programs, data formats, procedures, communication protocols, security policies, and public key cryptographic mechanisms
- PKI establishes a level of trust
- PKI is called a framework
- PKI provides authentication, confidentiality, nonrepudiation, and integrity of the messages exchanged

PKI

- PKI is a hybrid system of symmetric and asymmetric key algorithms
- The infrastructure contains the pieces that
  - Identify users
  - Create and distribute certificates
  - Maintain and revoke certificates
  - Distribute and maintain encryption keys
- Public key cryptography is one piece in PKI

PKI

- PKI is made up of many different parts
  - Certificate authorities
  - Registration authorities
  - Certificates
  - Keys
  - Users

PKI

- Each person who wants to participate in a PKI requires a digital certificate
- The certificate is created and signed by a trusted third party
  - Certificate authority (CA)
- Certificate binds the individual's identity to the public key
- CA signs the certificate to verify public key and identity

Certificate Authority

- A CA is a trusted organization that maintains and issues digital certificates.
- The registration authority (RA) verifies that individual's identity and passes the certificate request off to the CA
- CA can be internal to an organization
- CA can be external to an organization
  - Verisign

Certificates

- A certificate is the mechanism used to associate a public key with a collection of components that identify the owner.
- The standard for how the CA creates certificates is called X.509
- Dictates the different fields used in the certificate
- Certificate includes the serial number, version number, identity information, algorithm information, lifetime dates, and the signature of the issuing authority

Registration Authority

- The registration authority (RA) performs the certification registration duties.
  - The RA confirms the identity of an individual
  - The RA initiates the certification process with a CA
  - The RA cannot issue certificates

PKI Steps

- Steps to obtain a digital certificate
  1. John makes a request to the RA.
  2. The RA requests certain identification information
     - driver's license
     - phone number
     - address information
  3. RA sends his certificate request to the CA
  4. The CA creates a certificate with John's public key and identity information embedded.
     - private/public key pair is
     - private key is sent to him by secure means.
     - In most cases, user generates pair and sends public key during the registration process

PKI Steps

- John requests Mary's public key from a public directory.

5. The directory, sometimes called a repository, sends Mary's digital certificate
6. John verifies the digital certificate (CA digital signature) and extracts Mary's public key.
7. John uses Mary's public key to encrypt a session key that will be used to encrypt their messages
8. John sends the encrypted session key to Mary along with his certificate, containing his public key.

PKI Steps

9. When Mary receives John's certificate, her browser looks to see if it trusts the CA that digitally signed this certificate. If Mary's browser trusts this CA and verifies the certificate, both John and Mary can communicate using encryption.

Cryptography

- PKI may be made up of the following entities and functions:
  - CA
  - RA
  - Certificate Repository
  - Certificate revocation system
  - Key backup and recovery system
  - Automatic key update
  - Management of key histories
  - Time stamping

Applying Cryptography

FANSHAWE

Services of Cryptosystems

- PKI supplies the following security services:
  - Confidentiality
  - Access control
  - Integrity
  - Authentication
  - Nonrepudiation

Digital Signatures

- A digital signature is a hash value that has been encrypted with the sender's private key
  - The act of signing means encrypting the message's hash value with a private key
- The hashing function ensures the integrity of the message and the signing of the hash value provides authentication and nonrepudiation

Key Management

- Cryptography can be used as a security mechanism to provide:
  - Confidentiality Integrity and Authentication
- But only if the keys are kept secret
- Cryptography is based on trust
- Individuals must trust each other to protect their own keys
- Keys must be distributed securely to the right entities
- Keys must be updated or changed periodically

Key Management

- Keys should not be in available in clear text outside the cryptography device
- The key is what brings secrecy to encryption
- Key distribution and maintenance should be automated and hidden from the user
- Keys can be lost destroyed or corrupted therefore backup copies should be available and accessible when required

Key Management

- Rules for Keys and Key Management
  - Keys should be long
  - Keys should be random
  - The algorithm should use entire keyspace
  - Key's lifetime should correspond to sensitivity of data
  - Frequently used keys should have a shorter lifetime
  - Keys should be stored and transmitted securely
  - Keys should be properly destroyed when expired
  - Keys should be backed up or escrowed in case of emergencies

Cryptographic Attacks

- Passive Attack
  - Eavesdropping and sniffing data as it passes over a network are considered passive attacks because the attacker is not affecting the protocol, algorithm, key, message, or any parts of the encryption system
  - Passive attacks are hard to detect therefore try to prevent them instead
- Active Attack
  - Attacker is actually doing something instead of sitting back and gathering data.
  - Passive attacks are usually used to gain information prior to carrying out an active attack

Cryptographic Attacks

- Cipher-Only Attacks
  - The attacker has the cipher text of several messages
  - Attacker's goal is to discover the key used in the encryption process
  - Most common type of active attack
  - The hardest attack to actually be successful

Cryptographic Attacks

- Known-Plaintext Attacks
  - In known-plaintext attack the attacker has the plaintext and corresponding cipher text of one or more messages
  - Goal is to discover the key used to encrypt the messages so other messages can be deciphered and read
  - With plaintext and cipher text reverse-engineering, frequency analysis, and brute force can be used to determine key

Cryptographic Attacks

- Differential Cryptanalysis
  - This type of attack also has the goal of uncovering the key that was used for encryption purposes
  - Attack looks at cipher text pairs generated by encryption of plaintext pairs with specific differences and analyzes the effect and result of those differences
  - For example an attacker takes two messages of plaintext and follows the changes that take place to the blocks as they go through the different S-boxes.
    - Each message is being encrypted with the same key
  - The differences identified in the resulting cipher text values are used to map probability values to different possible key values

Cryptographic Attacks

- S-boxes
- Block ciphers use 4 bit substitution box (s-boxes)
- The s-box has the instruction or pattern on how the bits in the block are to be shifted or substituted

Cryptographic Attacks

- Linear Cryptanalysis
  - Linear cryptanalysis carries out functions to identify the highest probability of a specific key employed during the encryption process
  - Attacker carries out a known-plaintext attack on several different messages encrypted with the same key
  - Attacker evaluates the input and output values for each S-box
  - Evaluates the probability of input values ending up in a specific combination

Cryptographic Attacks

- Side Channel Attacks
  - Is the process of gathering information around the cryptosystem rather than a direct attack on it with the intention of discovering how it works, some critical information which will help in the discovery of the encryption key.

- Replay Attacks
  - An attacker captures some type of data and resubmits it with the hopes of fooling the receiving device into thinking it is legitimate information
  - Timestamps and sequence numbers are two countermeasures to replay attacks

Cryptographic Attacks

- Algebraic Attacks
  - Analyze the vulnerabilities in the mathematics used within the algorithm and exploit the intrinsic algebraic structure.
- Analytic Attacks
  - Identify algorithm structural weaknesses or flaws, as opposed to brute force attacks
- Statistical Attacks
  - Identify statistical weaknesses in algorithm design for exploitation
  - If statistical patterns are identified
  - The number of 0's compared to the number of 1's

Cryptographic Attacks

- Social Engineering attacks:
  - The goal is to trick the person to reveal they key or some sensitive information which can be used against them.
- Meet-in-the-Middle Attacks:
  - Refer to mathematical analysis – encrypting from one end and decrypting from the other, hence the meeting in the middle.

Cryptography Summary

- Cryptography is the science of protecting information by encoding it into an unreadable format
- Cryptography has been used in one form or another for over 4,000 years
- Encryption can be supplied at different layers of the OSI model
- Cryptosystem use many different algorithms

Summary

- A message can be *encrypted*
  - Which provides confidentiality.
- A message can be *hashed*
  - Which provides integrity.
- A message can be *digitally signed*
  - Which provides authentication, nonrepudiation, and integrity.
- A message can be *encrypted* and *digitally signed*
  - Which provides confidentiality, authentication, nonrepudiation, and integrity.
- Not all algorithms can provide all security services
  - Most of these algorithms are used in some type of combination to provide all the necessary security services required of an environment.

Homework

- Read the relevant chapter in the set book 'All In One CISSP Exam Guide' – by Shon Harris.
- 8th edition chapter 3 the section "Cryptography in Context" and the following sub sections.

- Earlier editions can be used but you will need to use the index to find the relevant sections.

- Then identify and do the practice m/c questions relating to this subject.

Questions

- ?