SENG 460

Practice of Information Security and Privacy

Cryptography

Cryptography Overview

- Cryptographic Concepts/Definition
- Security Cipher Properties & Principles
- Classical Ciphers & Modern Ciphers
- Cryptographic Applications/Systems
- Cryptographic Attacks

Cryptography Concepts/Definitions

- **Cipher/Algorithm:** Set of mathematical and logic rules used in cryptographic functions.
- **Encryption/Encipher:** Act of transforming data into an unreadable format.
- **Decryption/Decipher:** Act of transforming data into a readable format.
- **Key:** A secret that are used as the governing parameter in the acts of a cryptographic algorithm.
- **Keyspace:** All of the possible values under a specific key format.

Cryptography Concepts/Definitions

- **Plaintext/Cleartext:** A message/data in its original format.
- **Ciphertext /Crytogram:** A message/data in its encrypted format.
- **Transposition/Permutation:** The operations of shuffling or reordering the data in plaintext to hide original message.
- **Substitution:** The operations of replacing the data in plaintext to hide original message.
- **Avalanche effect:** The condition where small changes in the key or plaintext will significantly change the ciphertext.
- **Cryptanalysis:** Practice of uncovering flaws within cryptosystems.
- **Key clustering:** Instance when two different keys generate the same ciphertext from the same plaintext.

Cryptography Concepts/Definitions

- **Encoding:** The process of changing data into another format.
- **Decoding:** The process of changing an encoded data back into its original format.
- **One-way function:** A mathematical function that can be easily performed in one direction than in the other.
- **Collision:** An instance that a one-way function produces the same result on different inputs.

Security Cipher Properties

- **Diffusion**: Dissipate the statistical structure of the plaintext in the ciphertext
  - Good diffusion: small changes in the plaintext leads to significant change in the ciphertext
  - Can be accomplished by Transposition/Permutation operation
- **Confusion**: Complicate the relationship between the key and ciphertext
  - Good confusion: small changes in the key leads to significant change in the ciphertext
  - Can be accomplished by Substitution operation

Security Cipher Principles

- Auguste Kerckhoffs developed in 1883 six design principles for the military use of ciphers:
  - Cipher must be practically indecipherable
  - **Cipher itself must not be secret (arguable)**
  - **Key must be secret**
  - Applicable to telegraphic correspondence
  - Must be portable
  - Must be easy to use

Classical Ciphers

- Running Key Ciphers
- Concealment Ciphers
- Substitution Ciphers
- Transposition Ciphers
- One-time Pad (Vernam cipher)
- Product Ciphers

Classical Ciphers
- Running Key Ciphers

- Uses some physical components as the secret in the world around two communication parties.

149l6c7.299l3c7.911l5c8

Classical Ciphers
- Concealment Ciphers

- a message within a message.

“The saying, ‘The time is right’ is not cow language, so is now a dead subject.”

↓

key: every third word

↓

“The right cow is dead.”

- hiding data in another media type. (**Steganography)**

*Be aware of **digital watermark** when using some other’s logos!*

Classical Ciphers

- Substitution Ciphers

- Letters of plaintext are replaced by other letters or by numbers or symbols

Caesar Cipher: Replaces each letter by **nth** letter on. (such as 3^{rd})

"meet me after the toga party"

↓

"PHHW PH DIWHU WKH WRJD SDUWB"

Monoalphabetic Cipher : Each letter maps to a different random letter

Key: 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

↓ ↓ . . . . . .

D K V QFIBJWPESCXHTMYAUOLRGZN

Polyalphabetic Cipher : Each letter maps to a different random letter.

	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	T
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	T	U
W	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	D
X	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	C
Y	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	B
Z	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

Vigenere Table

Key: *SENG*

Enigma Machine

Classical Ciphers
- Transposition Ciphers

- hide the message by rearranging the letter order without altering the actual letters used.

Scytale cipher: used a sheet of papyrus wrapped around a wooden rod.

Row Transposition Ciphers: write letters of message out in rows over a specified number of columns, then reorder the columns according to some key before reading off the rows

Examples
Key: 3 4 2 1 5 6 7
Plaintext: „attack postponed until two am‟
Cipher: a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z
Ciphertext:
TTNAAPTMTSUOAODWCOIXKNLYPETZ

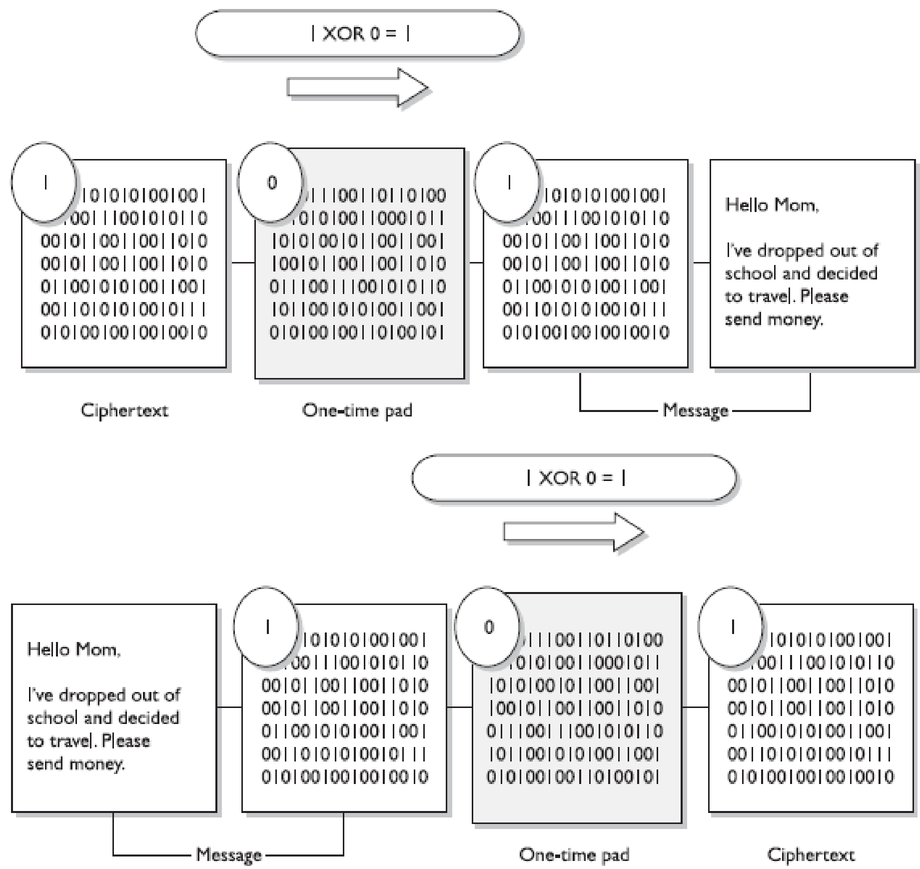
Rail Fence Cipher: write message letters out diagonally over a number of rows then read off cipher row by row.

Example:
–Plaintext: “meet me after the toga party”
–Key: write message out with a rail fence of depth 2:
m e m a t r h t g p r y
e t e f e t e o a a t
–Ciphertext: MEMATRHTGPRYETEFETEOAAT

Classical Ciphers
- One-time Pad

- Uses a pad which is made up of random values for encryption/decryption.

- Is considered to be unbreakable only if the following things are true about the implementation process:
  - *The pad must be used only one time.*
  - *The pad must be as long as the message*
  - *The pad must be securely distributed and protected at its destination*
  - *The pad must be made up of truly random values.*



Classical Ciphers
- Product Ciphers

- Ciphers using substitutions or transpositions are not secure because of language characteristics, using several ciphers in succession to make harder:
    - two substitutions make a more complex substitution
    - two transpositions make more complex transposition
    - a substitution followed by a transposition makes a new much harder cipher

Product Cipher forms the bridge from classical to modern ciphers.

Modern Ciphers

- **Symmetric Ciphers**
  - **Block Ciphers**
  - **Stream Ciphers**
- **Asymmetric Ciphers**
  - **Diffie-Hellman Key Exchange**
  - **RSA**

Modern Ciphers
- Symmetric Ciphers

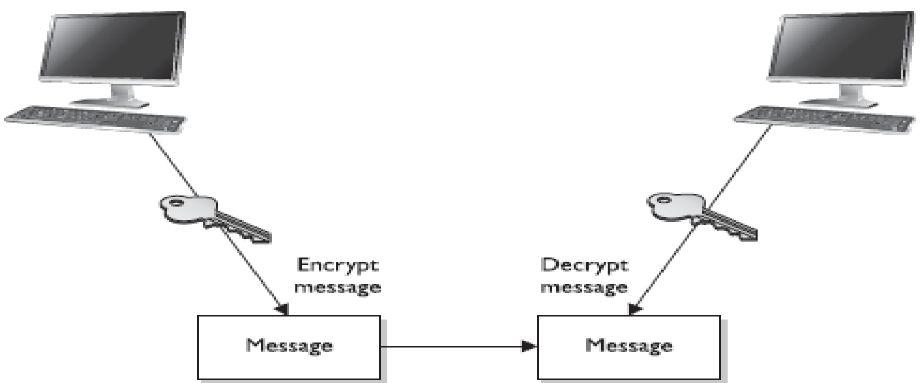
The sender and receiver use two instances of the same key for encryption and decryption:

Strengths

- Much faster (less computationally intensive) than asymmetric ciphers.

Weaknesses

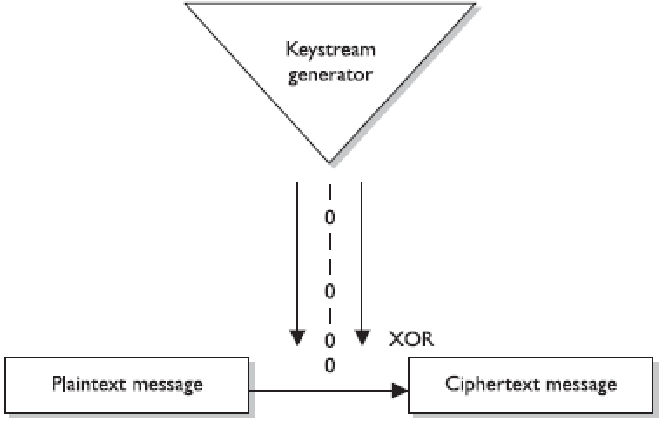
- Requires a secure mechanism to deliver keys properly.
- Each pair of users needs a unique key, possibly making key management overwhelming.
- Provides confidentiality but no nonrepudiation



Modern Ciphers
- Stream Ciphers

- Treats the message as a stream of bits and performs mathematical functions (usually **XOR** operation) on each bit individually.

- 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 the key
  - Statistically unbiased keystream (as many zeroes as ones)



Modern Ciphers

- A Stream Cipher Example: RC4

- A proprietary cipher owned by RSA DSI, simple but effective, widely used (web SSL/TLS, wireless WEP).
- Variable key size (from 40 to 2048 bits), byte-oriented stream cipher which forms random permutation of all 8-bit values.

Since RC4 is a stream cipher, must never reuse a key!

RC4 Implementation

```
/* Initialization */
For i = 0 to 255 do
S[i] =i;
T[i] = K[i mod keylen];

/* Initial Pemutation of S */
j = 0;
For i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap(S[i] , S[j]);
```

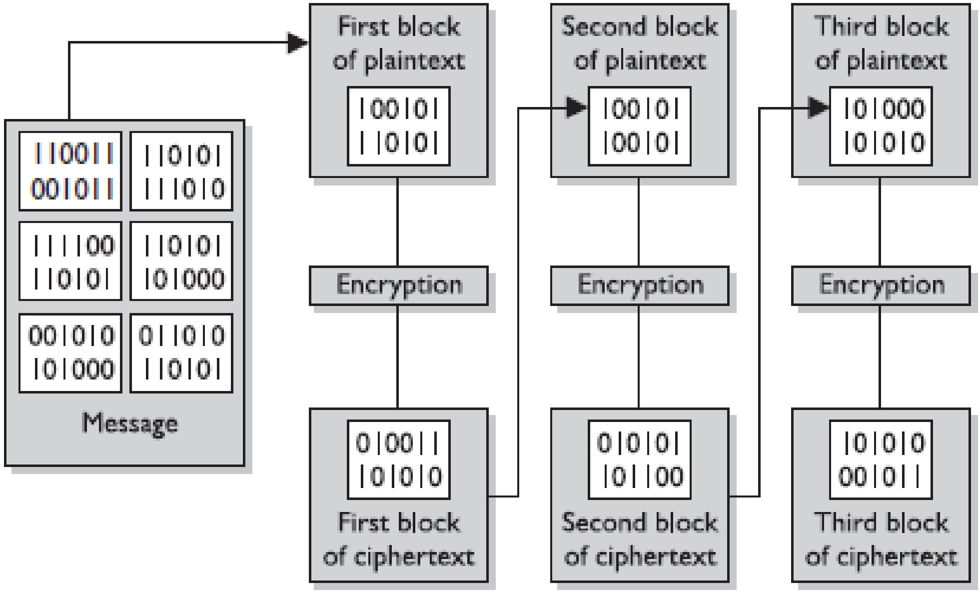
```
/* Stream Encryption */

i = j = 0
for each message byte Mi
i = (i + 1) (mod 256)
j = (j + S[i]) (mod 256)
swap(S[i], S[j])
t = (S[i] + S[j]) (mod 256)
Ci = Mi XOR S[t]
```

Modern Ciphers

- Block Ciphers

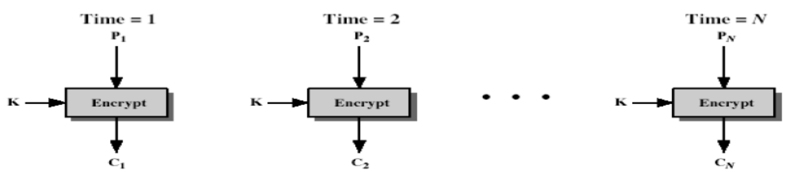
- The original message is divided into blocks of bits. These blocks are then put through mathematical functions one block at a time.



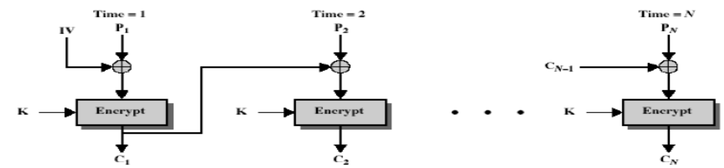
Modern Ciphers
- Block Ciphers

- Block ciphers have several modes of operation. Each mode specifies how a block cipher will operate.

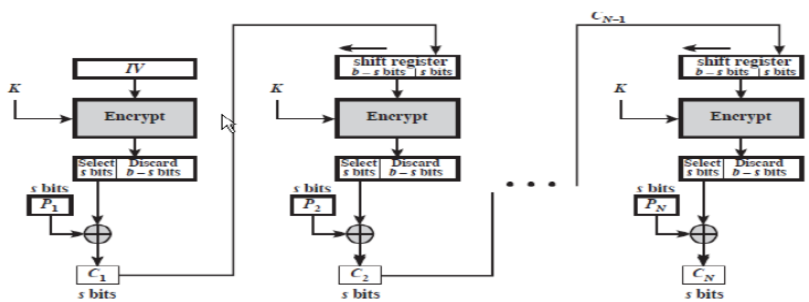
Electronic Code Book (ECB)



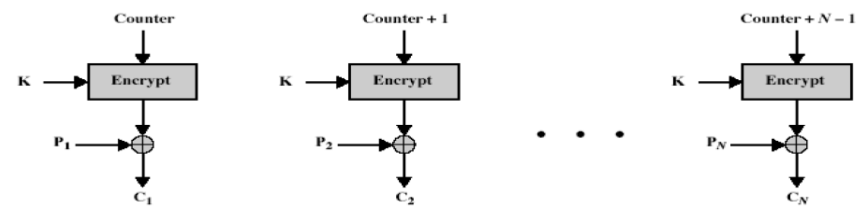
Cipher Block Chaining (CBC)



Cipher FeedBack (CFB)



Counter (CTR)

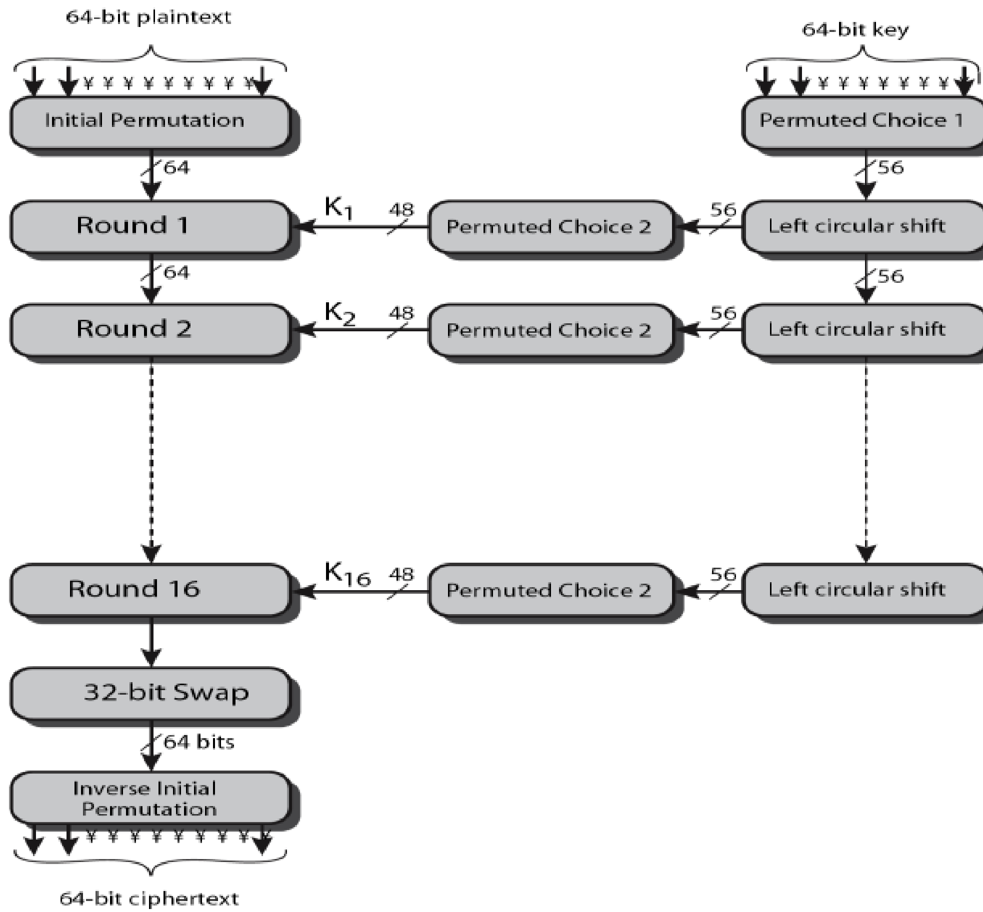


*To avoid two identical plaintexts that are encrypted with the same key create the same ciphertext, **Initialization vectors (IVs)** (which are random bits values) are usually used with keys. **IVS** do not need to be encrypted when being sent to the destination as it is usually dynamically generated for each encryption/decryption.*

Modern Ciphers

- A Block Cipher Example: DES

- Digital Encryption Standard (DES) is the most widely used block cipher in the world
- Most studied algorithm in existence
- Encrypts 64-bit data block using 56-bit key
- No discovery of fatal weakness in the algorithm itself
- 56 bits Key length is not considered secure any more today.



Modern Ciphers
- Advanced Encryption Standard (AES)

- US NIST issued call for new ciphers standard in 1997 to replace DES, 15 candidates accepted in Jun 1998, 5 were shortlisted in Aug 1999. **Rijndael** was eventually selected as the **AES** in Oct-2000.

- The block sizes that Rijndael supports are 128, 192, and 256 bits. The number of rounds depends upon the size of the block and the key length:
  - If both the key and block size are 128 bits, there are 10 rounds.
  - If both the key and block size are 192 bits, there are 12 rounds.
  - If both the key and block size are 256 bits, there are 14 rounds.

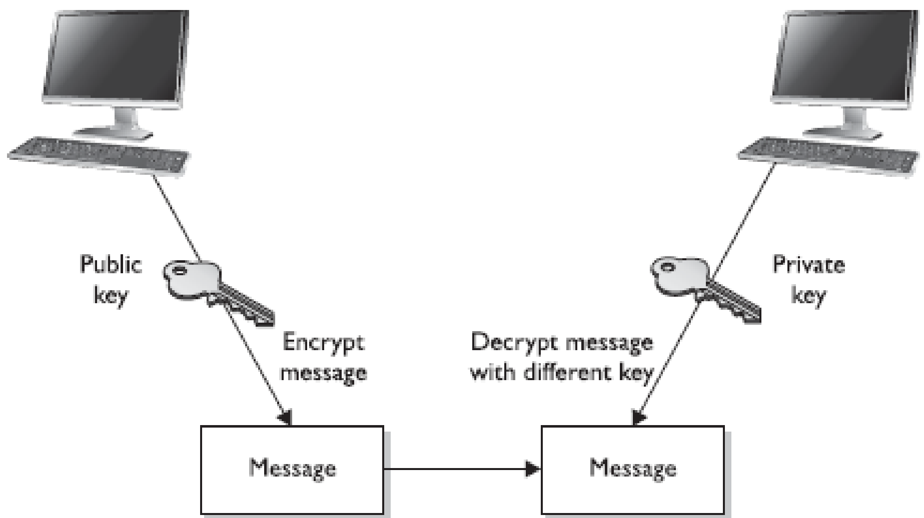
- Rijndael is now the algorithm required to protect sensitive but unclassified U.S. government information.

Modern Ciphers
- Asymmetric Ciphers

Two different asymmetric keys are mathematically related. If a message is encrypted by one key, the other key is required in order to decrypt the message. One key is usually made public called the ***public key,*** and the other must be known and used only by the owner , called the ***private key***.

Strengths
- Better key distribution than symmetric systems.
- Better scalability than symmetric systems
- Can provide authentication and nonrepudiation

Weaknesses
- Works much more slowly than symmetric systems



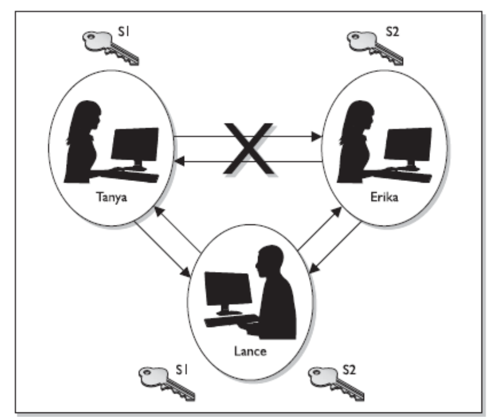
Modern Ciphers

- Diffie-Hellman Key Exchange

The **first** published asymmetric key algorithm, published by Diffie & Hellman in 1976. Diffie-Hellman is mainly used to establish a common key known only to the two communicating participants.

Diffie-Hellman Example

1. Alice & Bob who wish to swap keys agree on prime $q=353$ and $g=3$
2. select random secret keys:
   – A chooses $x_A=97$, B chooses $x_B=233$
3. compute respective public keys:
   – $y_A=3^{97} \bmod 353 = 40$ (Alice)
   – $y_B=3^{233} \bmod 353 = 248$ (Bob)
4. compute shared session key as:
   – $K_{AB}= y_B^{x_A} \bmod 353 = 248^{97} = 160$ (Alice)
   – $K_{AB}= y_A^{x_B} \bmod 353 = 40^{233} = 160$ (Bob)



Diffie-Hellman is vulnerable to Man in the Middle Attack!

Modern Ciphers
- RSA

RSA, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a public key algorithm that is the most popular and worldwide de facto standard for **encryption** and **authentication**.

RSA Key Setup

- Each user generates a public/private key pair by:
  1. select two large primes p, q at random
  2. compute their system modulus $n=p.q$
  3. compute $\varnothing(n)=(p-1)(q-1)$
  4. select at random an integer e
     1. where $1<e<\varnothing(n)$, $\gcd(e,\varnothing(n))=1$ (e and $\varnothing(n)$ are coprime)
  5. solve following equation to find another integer d
     1. Where $(e\cdot d) \bmod \varnothing(n) = 1$ and $0\leq d\leq\varnothing(n)$
- Publish the public key: PU={e,n}
- Keep secret the private key: PR={d,n}
- The key size refers to the length of the modulus n in bits

RSA Encryption/Decryption

- Encrypt a message M:
  - obtains public key of recipient $PU=\{e,n\}$
  - computes: $C = M^e \bmod n$, where $0\leq M<n$
- Decrypt the ciphertext C:
  - uses their private key $PR=\{d,n\}$
  - computes: $M = C^d \bmod n$

In RSA, public key {e,n} and private key {d,n} has a known relation as shown below. To know $\varnothing(n)$, has to factor n, If n is large enough, private key can be considered secure, currently assume 1024-2048 bit for n is secure.

$$(e\cdot d) \bmod \varnothing(n) = 1 \text{ and } 0\leq d\leq \varnothing(n)$$

Cryptographic Applications/Systems

- Cryptosystems provide confidentiality to ensure that the data cannot be read except by the valid recipient.
- Cryptosystems provide integrity by allowing valid recipients to verify that data has not been altered.
- Cryptosystems provide authenticity by providing the key to a valid user after that user is authenticated.
- Cryptosystems provide accountability by proving the origin of data, thereby preventing the sender from denying that he sent the message (**Nonrepudiation**).

Cryptographic Applications/Systems

- Message Integrity

Message integrity ensures that a message has not been altered

- Hash Functions
  - **MD5** produces 128 bits hash values, not considered secure anymore
  - **Secure Hash Algorithm (SHA1)** produces 160 bits hash values
  - **SHA-2** produces 224/256/384/512 bits hash values

- Message Authentication Code (MAC)
  - Hash MAC (HMAC): a keyed-hash value
  - Cipher block chaining MAC (CBC-MAC): the last block of encrypted message
  - Cipher-based MAC(CMAC): Similar with CBC-MAC, but with much better security ensurance.