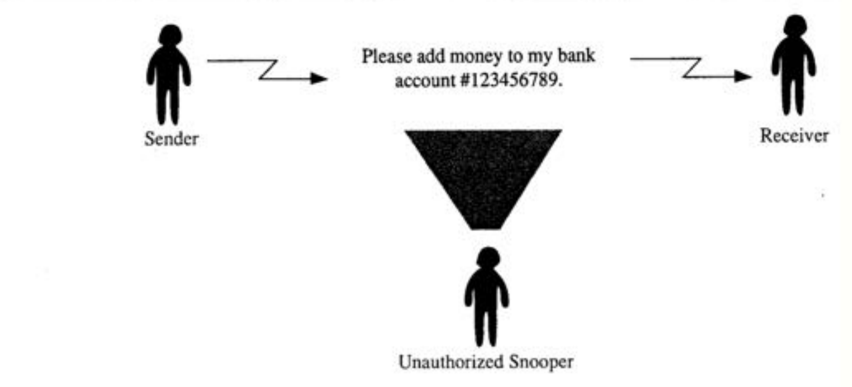
Overview

- Last Lecture
  - Data Integrity 2
- This Lecture
  - Data Security 1
  - Source: Sections 31.1, 31.2
- Next Lecture
  - Data Security 2
  - Source: Sections 31.2-31.3

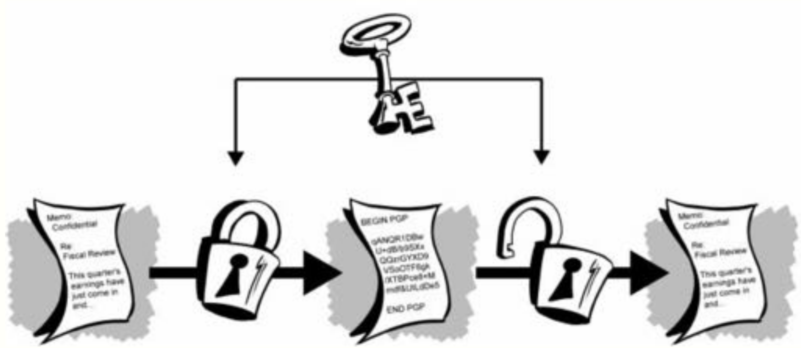
Figure 4.12 Sending Unsecured Messages



Introduction

(demo video: Encryption and decryption)

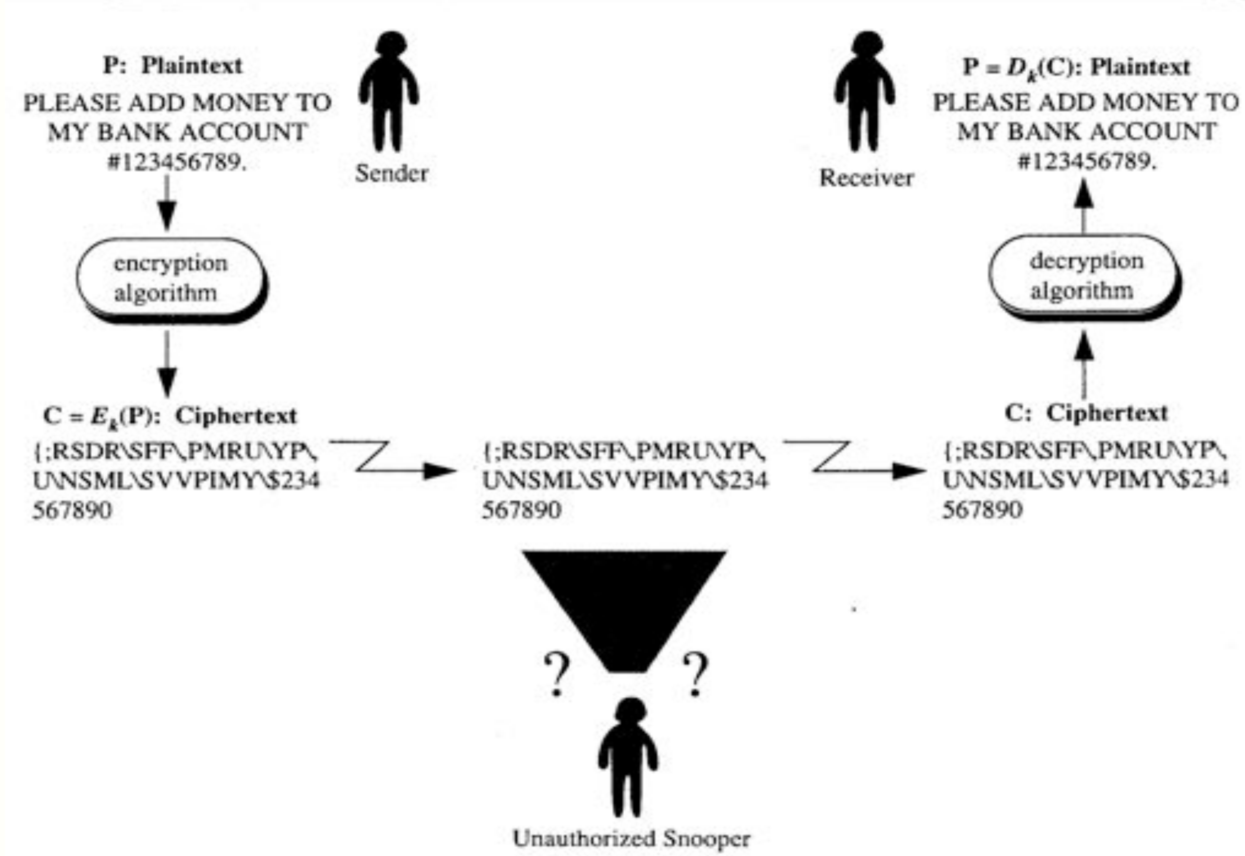
- Data security
  - How to prevent someone else from knowing the contents of a message while it is being transmitted
- Encryption - transform information into a different, unintelligible form
- Decryption - restore the original information from the encrypted form
- Plaintext - original data
- Ciphertext - encrypted data



Example

P - plaintext
C - ciphertext
E – encryption algorithm
D - decryption algorithm
k, k' - keys
$C = E_k(P)$
$P = D_{k'}(C)$
$P = D_{k'}(E_k(P))$

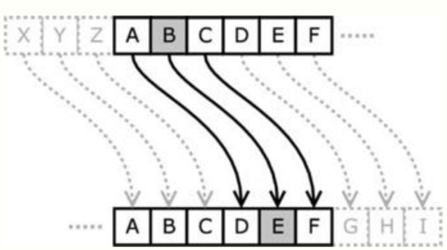
Figure 4.13 Sending Encrypted Messages

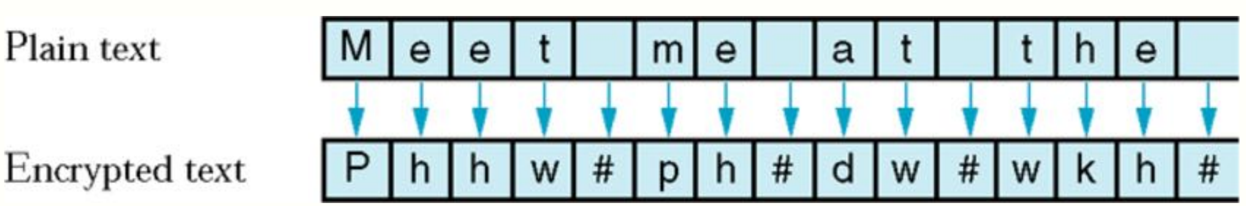


Caesar Cipher

(demo video: Caesar Cipher)

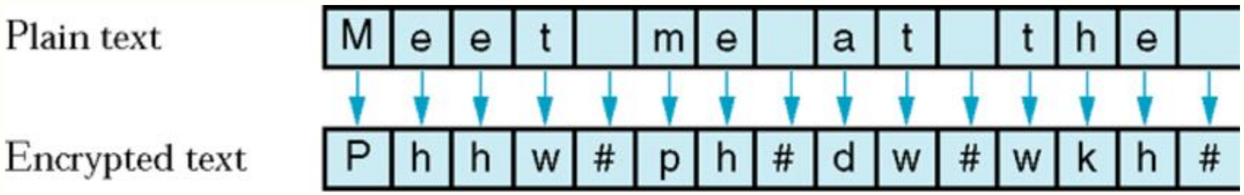
- Shift of character values
  - Example: A = A + 3, B = B + 3,… for ASCII
  - Decrease each code by 3 to decrypt it
  - What is the key?
- Various keys can be used
  - E.g. shift to the next character on the keyboard





Problems with Caesar Cipher

- Easy to break by guessing frequently occurring letters
  - E, T, O A, N, and space are frequently used.
  - If you can guess the space character, then you can have a go at guessing short words such as 2-4 character words.
  - Probable patterns can help.
    - TO, THE, OF, etc.



Polyalphabetic Cipher

- Idea is to change the letter frequency so a given plaintext character is not always replaced by the same ciphertext character.
- Create an alphabet matrix as shown on the next slide.
- Let i be the position of a given character in the plaintext message.
- Let j be the position of a given character in the alphabet
- Replace the character with M[(i mod 26), j]

Polyalphabetic Cipher (cont.)

(demo video: Turkey)

Key for Vigenère Cipher

row 0:	A	B	C	D	E	F	G	H	I	J	K	L	$\boxed{M}$	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
row 1:	B	C	D	E	$\boxed{F}$	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
row 2:	C	D	E	F	$\boxed{G}$	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
row 3:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	$\boxed{W}$	X	Y	Z	A	B	C
	⋮																⋮									
row 24:	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
row 25:	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

Example

- Example
  - Plaintext: ….THE ….THE…THE
  - Assume the first THE starts at position 25, the second THE starts at position 54, and the third THE starts at position 104
  - Ciphertext: …SHF…VKI…TIG

Example (cont.)

Table 4.3 Letter Substitutions Using the Vigenère Cipher

Plaintext Letter	i = (Relative position in message)	i mod 26	j Relative position in alphabet	Ciphertext Letter
T	25	25	19	S
H	26	0	7	H
E	27	1	4	F
T	54	2	19	V
H	55	3	7	K
E	56	4	4	I
T	104	0	19	T
H	105	1	7	I
E	106	2	4	G

[*] It also assumes that the letters correspond to consecutive binary codes such as in the ASCII code.

Polyalphabetic Cipher (cont.)

Key for Vigenère Cipher

row 0:	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
row 1:	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
row 2:	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
row 3:	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
⋮	⋮
row 24:	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
row 25:	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

Problems of Polyalphabetic Cipher

- Can break by using some clues
  - Letters in TIG are alphabetic successors to the letters in SHF
  - S and H, V and K, T and I all have the same difference

Transposition Cipher

- Idea: Rearrange the plaintext of a message.
- Step1: Store the plaintext message in a 2 dimensional array.
- Step2: Send the columns out of order.
- Example :
  - Message: MISS PIGGY KERMIT ANIMAL AND FOZZIE BEAR
  - Send columns 2, 4, 3, 1, 5
  - IIKTMNZBSGRAL IASGE ADZEMP IIAO YMN FER is sent

COLUMN NUMBERS				
1	2	3	4	5
M	I	S	S	
P	I	G	G	Y
	K	E	R	M
I	T		A	N
I	M	A	L	
A	N	D		F
O	Z	Z	I	E
	B	E	A	R

Problems of Transposition Cipher

- Letter frequencies are preserved.
- Letter frequencies matches what we expect.
  - Implies substitution was not used
  - Hints that a transposition cipher was used
- Try column arrangements yielding common sequences such as ING, THE, IS . . .

Bit-Level Cipher

- Not all data are characters
- Define a bit pattern as an encryption key.
- Perform an XOR between the data and key.
- Send the result.
- To decrypt, perform the same process

Figure 4.16 Encryption Using Exclusive OR Bit Operation

1101100101001	Plaintext
1001011001010	Encryption key
0100111100011	Ciphertext = plaintext exclusive-or'd with the encryption key
1001011001010	Decryption key (same as the encryption key)
1101100101001	Plaintext = ciphertext exclusive-or'd with the decryption key

Problems with Bit-Level Cipher

- Short keys may result in repeated substrings
  - Helps break pattern
- One time pad
  - Each key is used only once
  - Extreme case - Key length is equal to the original string length
  - Distribution of keys is difficult

Questions?

- Substitutions: Caesar/Polyalphabetic cipher
- Transpositions: Transposition cipher
- exclusive-OR operations: Bit-level cipher
- What is most important for Encryption
  - Good Locks! (Simple vs. Complex Encryption Algorithms)
  - Nice Keys! (Short vs. Long keys)
  - such that the Hackers can not break it!

Drawbacks of Traditional Encryption

- Methods so far are not very complex.
- With short keys, they are not good and contain clues to aid in breaking the code.
- Longer keys makes the ciphertext more cryptic, but distribution of keys (especially large ones) is unwieldy.
- An alternative approach uses shorter keys but more complex procedures - DES

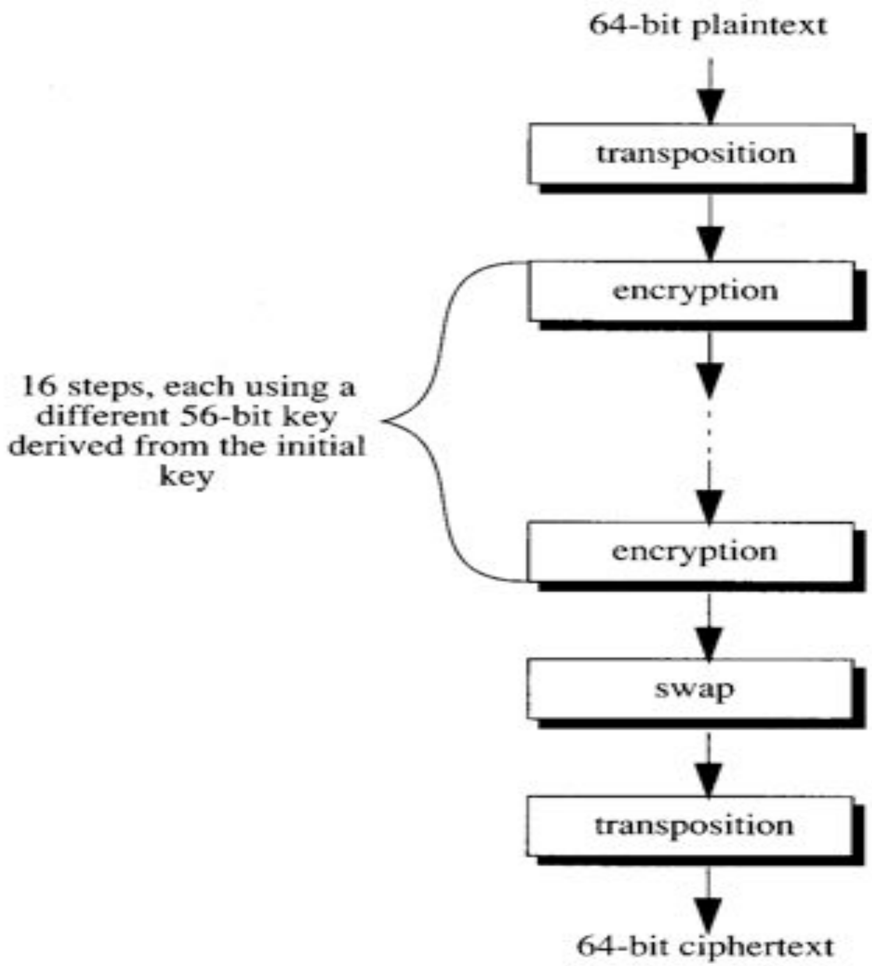
DES (Data Encryption Standard)

- Developed by IBM in the early 1970's
- Adopted as a standard by US government in 1977 for all commercial and non-classified use
- Divided into 64-bit blocks, uses a 56-bit key
- The algorithm is a complex combinations of transpositions, substitutions, exclusive-OR operations, and other processes to produce 64 bits of encrypted data.

DES (cont.)

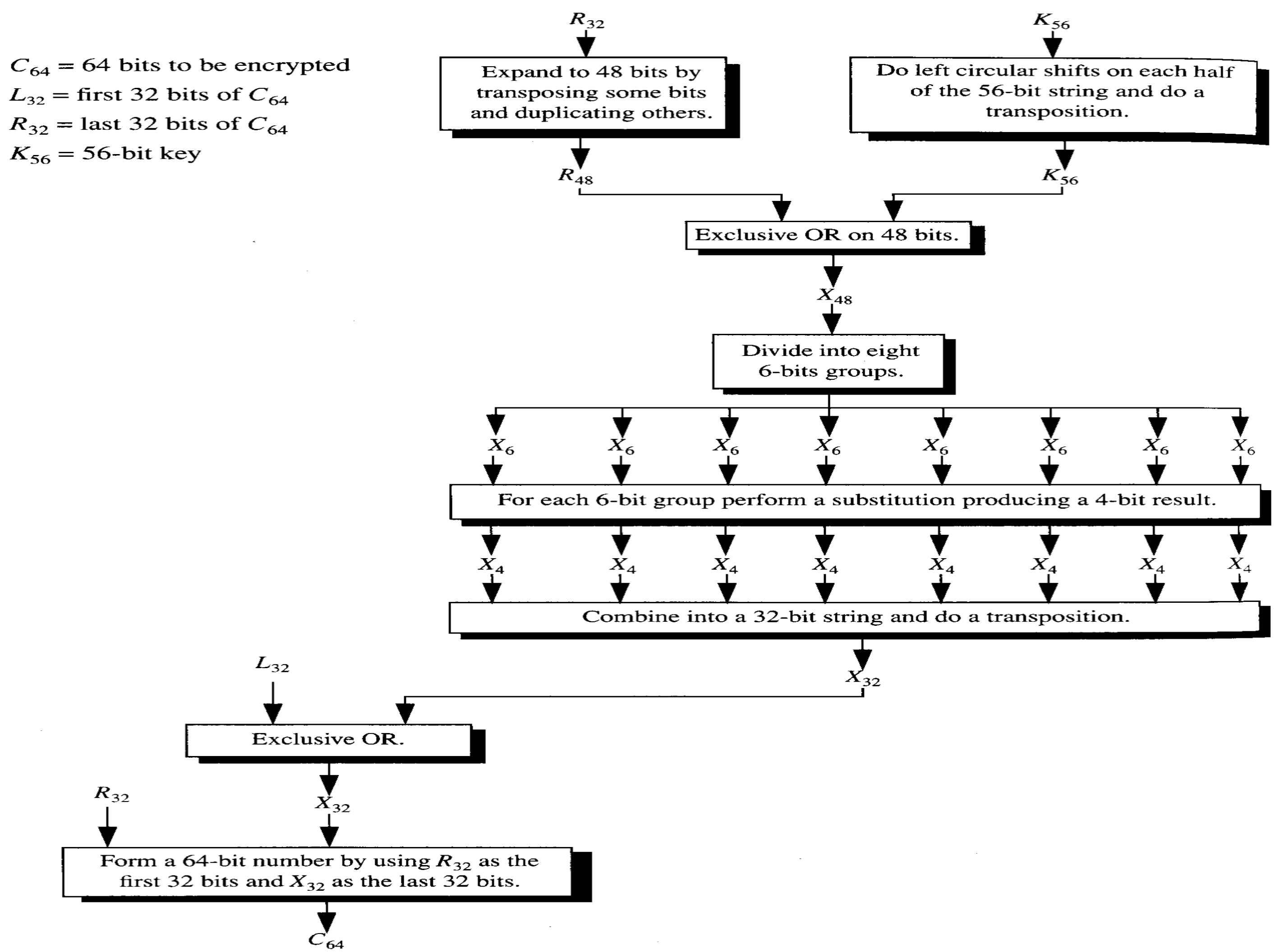
demo: http://www.formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng.swf
https://www.youtube.com/watch?v=H2LlHOw_ANg

Figure 4.17 Outline of the DES



One Step of DES

Figure 4.18 One of Sixteen Encryption Steps of the DES



Worries Behind DES

- Some say it is not sufficiently secure
  - Some think it can be broken in a few hours on a massively parallel computer
- IBM originally used a 128-bit key.
- The National Security Agency (NSA) asked for it to be changed to 56-bits without public explanation
  - Guess: easy for NSA to break?
- 56-bit key is relatively short and has $2^{56} \approx 7 * 10^{16}$ possible key values
- The rationale behind the substitutions in the algorithm were never fully explained

DES Cracker

https://en.wikipedia.org/wiki/EFF_DES_cracker

- DES uses a 56-bit key- 2^{56} possible keys
- One of the major criticism of DES was that the key size was too short
- In 1998, the EFF built “DES Cracker” for $250,000
- brute force search of DES cipher's key space
- 1998, DES Challenge II – 56 hours of work, winning $10,000
- 1999, DES Challenge III — 22 hours and 15 minutes, winning another $10,000
- DES: the key-space is relatively small

Variations of DES

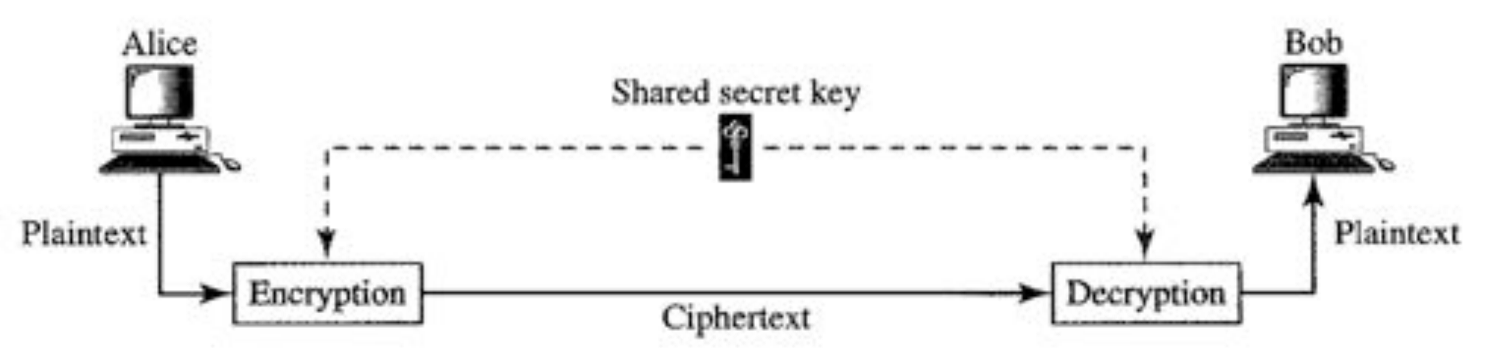
- Triple-DES (3DES)
  – Uses the DES encryption algorithm three times with two different keys
  – Used by financial institutions to extend the life of DES
  – Increased the key size: 3*56=168-bit, but too slow
- AES (Advanced Encryption Standard)
  – Announced as a standard in 2002 and now used worldwide

Table 30.1 *AES configuration*

Size of Data Block	*Number of Rounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

Private Key Encryption

- Symmetric-key: the same key (<u>Secret key</u>) is used by the sender and receiver. The key is shared.
  - Caesar cipher, Transposition ciphers, DES introduced in this lecture
  - Key is very important in these methods. The secrecy of the key must be protected
  - These methods are called private key encryption



Private Key Encryption

- The best encryption method in the world is no good if the key cannot be kept secret.
- How does the sender communicate the key to the receiver?
  - Sender send the key: what if an unauthorized receiver gets it?
  - Encrypt the key: same problem?
  - Can we make the encryption key public while still making the encrypted message secure? (next lecture)

Summary

- Principles of encryption and decryption
- Functional expression
- Caesar cipher
- Polyalphabetic cipher
- Transposition cipher
- Bit-level cipher
- DES