

ISA 666 Internet Security Protocols

Secret Key Cryptography

ISA 666

1

Agenda

- A little History & Basics
- Generic Block Cipher
- DES
- Modes of Block Ciphers
- Multiple Encryptions

ISE at George Mason University

ISA 666

2

A Little History

ISA 666

3

A little History

- Cryptography was first used for **Secrecy (Confidentiality)** ... now evolved to include **Integrity, Authentication & Authenticity**, and in some cases **Non-Repudiation**.
- Written on bold head
- **Scytale encryption** – Uses paper or leather and is wrapped around a rod (cylinder)



ISE at George Mason University

ISA 666

4

Some Trivial Codes

- Running Key Cipher
 - Doesn't use mathematical formulas, instead everyday items.
 - For example a set of books
 - Numbers are sent representing book number, page number, line number, and word number.

ISE at George Mason University

ISA 666

5

Some Trivial Codes

- Caesar cipher: substitution cipher:
 - Replace each letter with the one 3 letters later
 - $A \rightarrow D, B \rightarrow E$
 - For example: GMU \rightarrow JPX
- Captain Midnight Secret Decoder rings:
 - shift variable by n : IBM \rightarrow HAL
 - How many possibilities?

only 26 possibilities

ISE at George Mason University

ISA 666

6

Some Trivial Codes

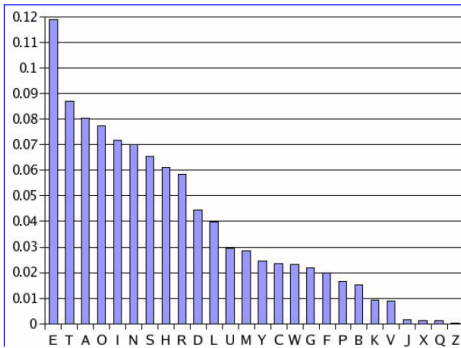
- Mono-alphabetic cipher:
 - generalization, arbitrary mapping of one letter to another
 - $26!$, approximately 4×10^{26}
 - How can it be cracked?

Using statistical analysis of letter frequencies

The problem: Letter Frequencies (I)

- English is highly redundant, as shown in the next slide, it has a non-uniform distribution of letters.
- Each symbol of ciphertext depends on only one symbol of plaintext and one value of the permutation key, so guessing part of the key gives part of the plaintext.
- Attack proceeds by guessing parts of key corresponding to most common letters, which makes it possible to decipher entire message.

The problem: Letter Frequencies (II)



Possible solutions

- You can try not to use redundant letters, like the letter “e”, as was done by a French writer named Georges Perec in 1969. He published a 300-page novel *La Disparition* (The Disappearance). It was translated into English by Gilbert Adair and is called “A Void”.
- Or you can group the plaintext into blocks that will then go through some transformation.

Some Trivial Codes (cont'd)

- Poly-alphabetic Ciphers
 - A set of related mono-alphabetic substitution rules is used
 - A key determines which particular rule is chosen for a given transformation
- Vigenere Cipher is an good example
 - uses a table together with a keyword to encipher a message.
 - History: Proposed by Blaise de Vigenere from the court of Henry III of France in the sixteenth century. This guy was a diplomat @ the age of 17

Vigenere Cipher

	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	V
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	W
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	X
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

Class Exercise using Vigenere Cipher

- Plaintext: H A R D
- Key-word: X A B V
- Ciphertext:

Class Exercise using Vigenere Cipher

- Plaintext: H A R D
- Key-word: X A B V
- Ciphertext: **E A S Y**

Xor Basics

- Modern cryptosystem operates on bits using addition mod 2, rather than letters using addition mod 26, as the basic units of a message.
- The operation is written as \oplus . So:

$$0 \oplus 0 = 0, 1 \oplus 1 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1$$

- This is the same as the logical exclusive OR of two bits. We can extend this operation to sequence of bits, so:

$$u \oplus v = w$$

- Here w is the bitwise exclusive OR of u and v . For example:

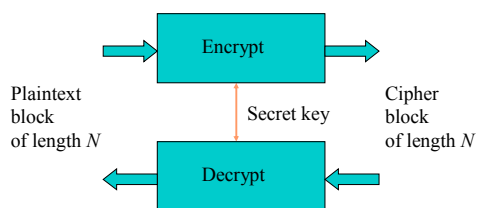
$$0011 \oplus 1010 = 1001$$

- Any w of bits, $w \oplus w$ is a string of zeroes, so for any strings u and v of the same length, we get:

$$u \oplus v \oplus v = u$$

Generic Block Cipher

Generic Block Cipher



Generic Block Encryption (Cont'd)

- Convert one block to another: **one-to-one**
- Block should be long enough to avoid known-plaintext attack, but not too long (performance).
 - 64 bit typical
- Key should be long enough to defeat brute-force attack
- Output should look random
 - No obvious correlation between plaintext and ciphertext
 - Bit spreading

Generic Block Encryption (Cont'd)

- By substitution:
 - Need to know how to substitute each plaintext message.
 - How many bits are needed for specifying random substitution of k -bit blocks: $k \cdot 2^k$ bits
 - Why?
 - There are 2^k possible bit sequences of length k .
 - For each one, need to specify a bit vector of length k .
 - Not Practical for large block sizes of say.. 64 bit
 - There will 2^{64} possible input values and for each one we have to specify a 64-bit output value.
 - Since there are 2^{64} different possible permutations of 2^{64} values, it need more than 2^{69} bit to represent.

Generic Block Encryption (Cont'd)

- By Permutations:
 - Need to know which position each bit is placed.
 - How many bits are needed for specifying random permutation of k -bit blocks = $k \cdot \log_2 k$
 - How many possible position does each bit have = $k (1..k)$
 - How many bits are needed to encode k positions = $\log_2 k$

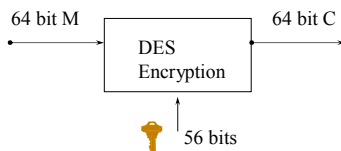
DES (Data Encryption Standard)

DES (Data Encryption Standard)

- DES is a widely-used method of data encryption using a (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries.
- There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys.
- Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.
- It was developed in the 1970s by the National Bureau of Standards with the help of the National Security Agency. Its purpose is to provide a standard method for protecting sensitive commercial and unclassified data.
- IBM created the first draft of the algorithm, calling it LUCIFER. DES officially became a federal standard in November of 1976, it expired in 1998 (22 years old) .

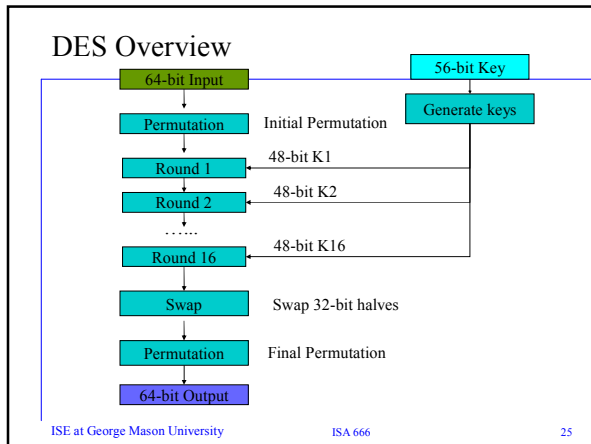
DES (Data Encryption Standard)

- Key: 64 bit quantity=8-bit parity+56-bit key
 - Every 8th bit is a parity bit.
 - From these 56 bits, 16 48 bit sub-keys are created.
- 64 bit input, 64 bit output.

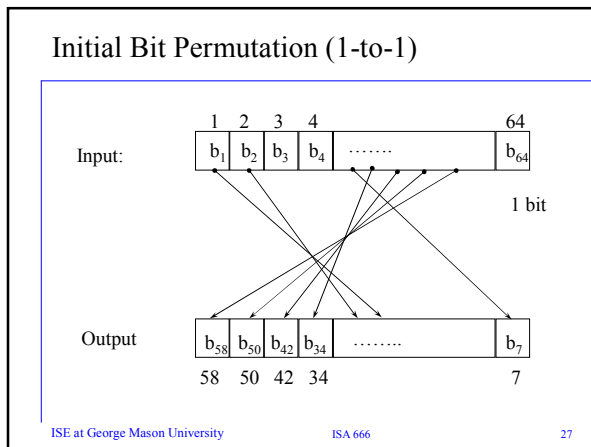


Demo Time

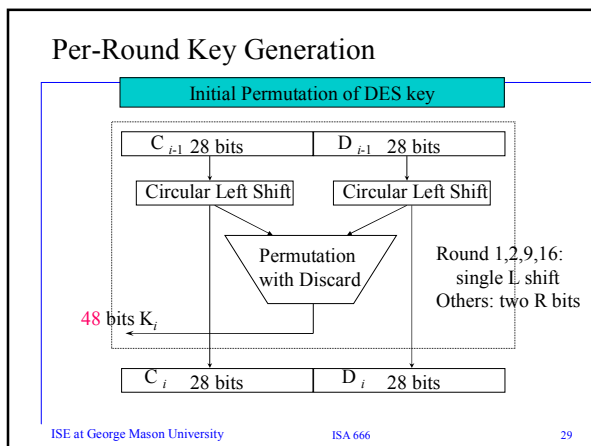
- The Demo is a summary of the next 15 slides.



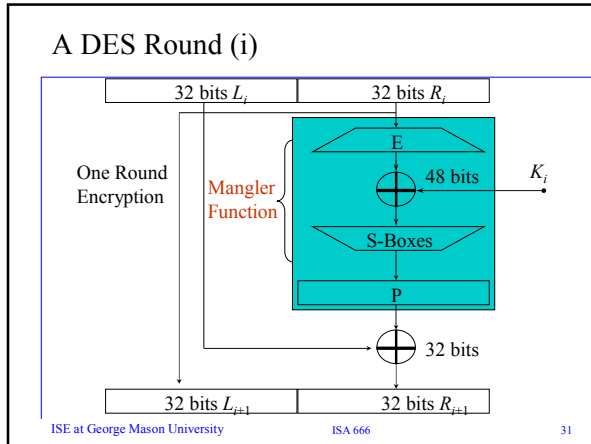
- ### Initial and Final Permutations
- Initial permutation (IP)
 - View the input as M : 8×8 bit matrix
 - Transform M into $M1$ in two steps
 - Transpose row x into column $(9-x)$, $1 \leq x \leq 8$ (equivalent to 90° clockwise turn of the matrix)
 - Apply permutation on the rows:
 - For even row y , it becomes row $y/2$
 - For odd row y , it becomes row $(5+y)/2$
 - Final permutation $FP = IP^{-1}$
 - Why?
- ISE at George Mason University ISA 666 26



- ### Per Round Key Generation
- Initial Key has 64 bits
 - Remove Every 8th bit:
 - Remove 8, 16, 24, 32, 40, 48 (parity check)
 - End up with 56 bits:
 - Now do an initial permutation of the 56 bit key:
 - First half (28 bits) = C_0
 - Second half (28 bits) = D_0
- ISE at George Mason University ISA 666 28

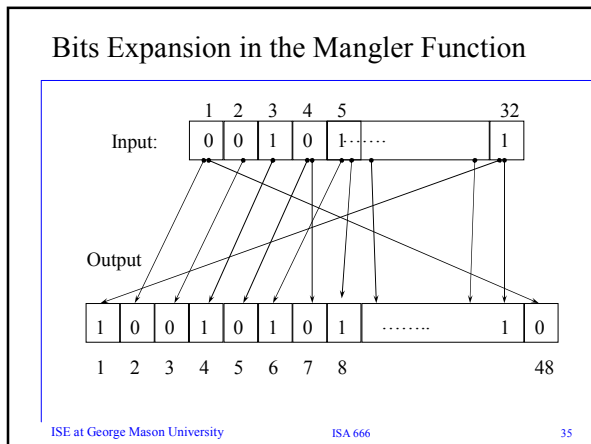
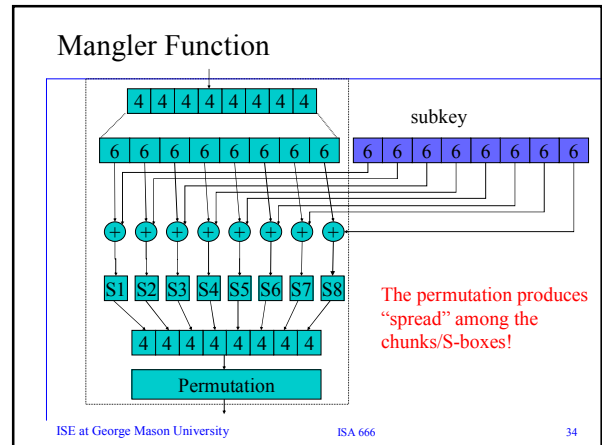


- ### Round (i)
- 64 bit input broken down into two halves
 - L_i and R_i (32 bits each)
 - Recursively define:
 - $L_{i+1} = R_i$
 - $R_{i+1} = \text{mangler}(R_i, k_n)(+)L_i$
- Pictorially
- ISE at George Mason University ISA 666 30



- ### Important Properties of DES Round
- The decryption in a DES round does NOT require the mangler function to be reversible!
 - The decryption of 64 bit block in a DES round is equivalent to encryption of the 64 bit block (by swapping the 32 bit halves) with the same key
 - if $E(L_i, R_i, K_i) = (L_{i+1}, R_{i+1})$, then
 - $D(L_{i+1}, R_{i+1}) = E(R_{i+1}, L_{i+1}, K_i) = (R_i, L_i)$
 - Why?
- ISE at George Mason University ISA 666 32

- ### Answer
- Reverse the i^{th} step = compute L_{n+1} and R_{n+1} from L_n and R_n
 - Suppose we know L_{n+1} and R_{n+1} , then:
 - $R_n = L_{n+1}$
 - Know $R_{n+1} = \text{mangler}(R_n, k_n)(+)L_n$
 - Compute $\text{mangler}(R_n, k_n) = \text{mangler}(L_{n+1}, k_n)$
 - Then $L_n = \text{mangler}(R_n, k_n)(+)R_{n+1}$
- ISE at George Mason University ISA 666 33



E Box of DES

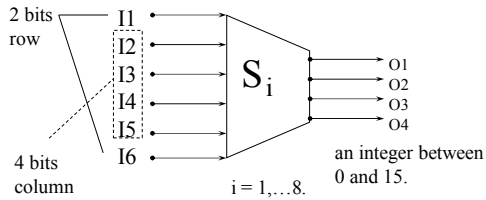
- How is the E Box defined?

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

ISE at George Mason University ISA 666 36

S-Box (Substitute and Shrink)

- 48 bits \implies 32 bits. ($8 \times 6 \implies 8 \times 4$)
- 2 bits used to select amongst 4 permutations for the rest of the 4-bit quantity



ISE at George Mason University

ISA 666

37

S-Box (Cont'd)

Each row and column contain different numbers.

	0	1	2	3	4	5	6	...	15
0	14	4	13	1	2	15	11	
1	0	15	7	4	14	2	13	
2	4	1	14	8	13	6	2	
3	15	12	8	2	4	9	1	

Example: input: **100110** output: ???

ISE at George Mason University

ISA 666

38

DES Standard

- | | |
|--|---|
| <ul style="list-style-type: none"> • Cipher Iterative Action <ul style="list-style-type: none"> - Input: 64 bits - Key: 48 bits - Output: 64 bits | <ul style="list-style-type: none"> • Key Generation Box <ul style="list-style-type: none"> - Input: 56 bits - Output: 48 bits |
|--|---|

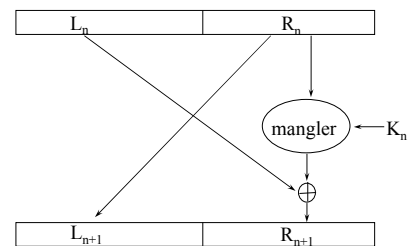
One round (Total 16 rounds)

ISE at George Mason University

ISA 666

39

Feistel Cipher Encryption

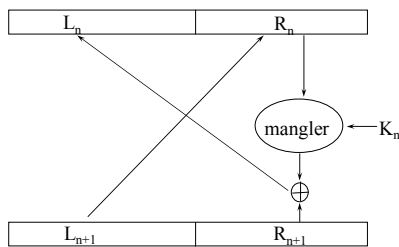


ISE at George Mason University

ISA 666

40

Feistel Cipher Decryption



ISE at George Mason University

ISA 666

41

Avalanche Effect

- A small change in either the plaintext or the key should produce a significant change in the ciphertext.
- DES has a strong avalanche effect.
- Example
 - Plaintexts: 0X0000000000000000 and 0X8000000000000000
 - Same key: 0X016B24621C181C32
 - 34 bits difference in cipher-texts
 - Similar result with same plaintext and slightly different keys

ISE at George Mason University

ISA 666

42

Concerns About DES

- Key space problem: 56 bit key (2^{56})
 - DESCHALL recovered RSA challenge I key on June 17, 1997 (6 month into the contest)
 - \$.25m (total cost), July 15, 1998, RSA DES challenge II key recovered in 56 hours
- Cryptanalysis
 - Sixteen Weak and semi-weak keys:
 - Differential cryptanalysis require less tries using chosen plaintext/ciphertext [Biham, 1993]
 - Effective up to 15 rounds
 - DES is well designed to defeat differential analysis
 - Linear cryptanalysis requires only known plaintext/ciphertext [Matsui, 1993]

DES Summary

- Simple, easy to implement:
 - Hardware/gigabits/second,
 - software/megabits/second
- 56-bit key DES maybe acceptable for non-critical applications but triple DES (3-DES) should be secure for most applications today
- Supports several operation modes: ECB CBC, OFB, CFB

Rijndael Demo

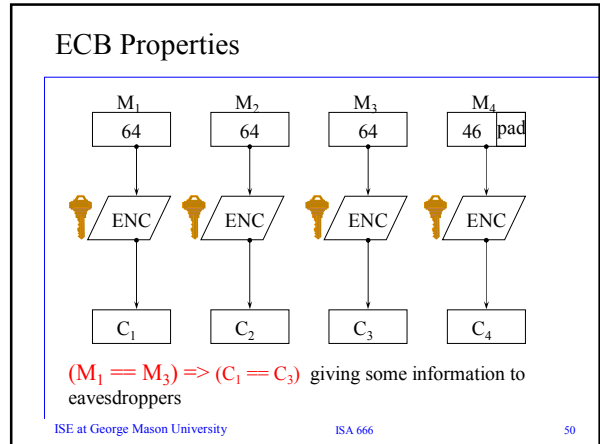
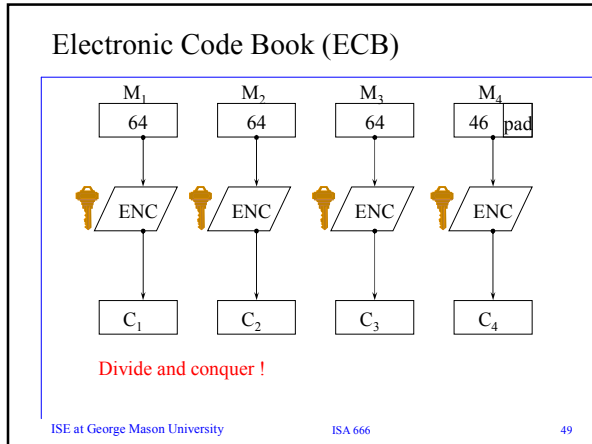
Modes of Block Cipher Operations

Encrypting a Large Message

- Modes of block cipher operations
 - ECB (Electronic Code Book)
 - CBC (Cipher Block Chaining Mode)
 - OFB (Output Feedback Mode)
 - CFB (Cipher Feedback Mode)

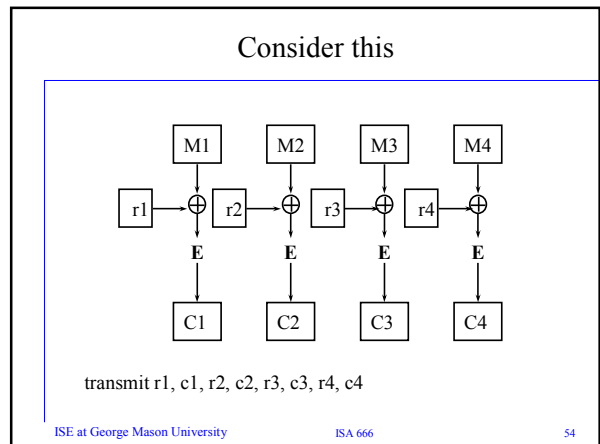
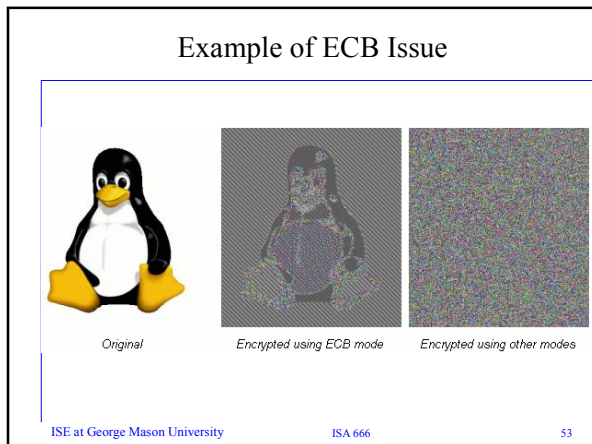
Encrypting Large Messages

- The basic algorithms encrypt a fixed size block
- Obvious solution is to encrypt a block at a time. This is called Electronic Code Book (ECB)
- Repeated plaintext blocks yield repeated ciphertext blocks
- Other modes “chain” to avoid this (CBC, CFB, OFB)
- Encryption does not guarantee integrity!



- ### ECB Properties (Cont'd)
- Cipher block substitution and rearrangement attacks
 - fabrication of specific information
 - Advantage: No error propagation.
 - **Two serious flaws, one advantage!**
- ISE at George Mason University ISA 666 51

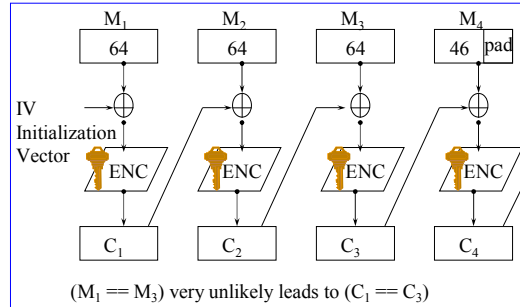
- ### ECB Properties (Cont'd)
- Disadvantage:
- If $c_i=c_j$, then you know $p_i=p_j$
 1. Can reorder blocks
 2. Can substitute (fabricated information) blocks to affect plaintext
 - Salary Example
- Advantage:
- Advantage: No error propagation.
- Two serious flaws, one advantage!**
- ISE at George Mason University ISA 666 52



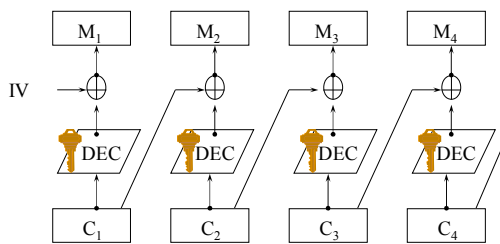
Problems with previous slide

- Need to send twice as much data
- Can still rearrange blocks
- If two ciphertext blocks are equal, you know XOR of two plaintext blocks = XOR of the corresponding two random numbers
- CBC generates its own “random numbers” by using previous ciphertext block, plus one additional block (the “IV”, initialization vector)

Cipher Block Chaining (CBC)



CBC Decryption

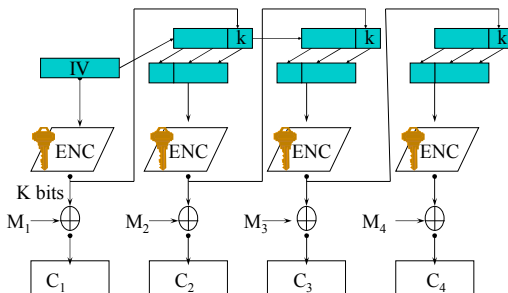


CBC Properties

- Chaining dependency
 - Each ciphertext block depends on all preceding plaintext blocks
 - To change a particular bit in m_i , change the corresponding bit in c_{i-1} . The side effect is that m_{i-1} will be garbled.
- Error propagation
 - Each error in c_j affects decipherment of m_j and m_{j+1} .
- Error recovery
 - An error in c_j doesn't propagate beyond c_{j+1} .
 - Can recover from loss of cipher text blocks.

Output Feedback Mode (OFB)

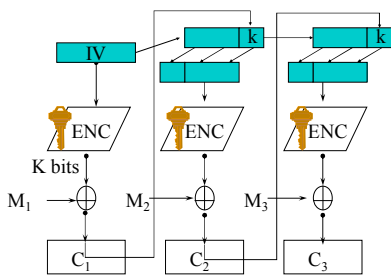
Like a Random Number Generator...



OFB Properties

- (OFB) stream generated:
 - IV (transmitted in the clear)
 - $pad_1 = e(IV, key)$
 - $pad_2 = e(pad_1, key)$
 - $pad_i = e(pad_{i-1}, key)$
- Chaining dependencies
 - Key stream is plaintext-independent
 - Allow pre-computing of pseudo-random stream (One-Time Pad); XOR can be implemented very efficiently
- No error propagation problem as in CBC
- What if ciphertext is garbled or lost?
 - If garbled, only those plaintext bits are garbled.
 - If lost or duplicated, you lose synchronization so you're hoses.

Cipher Feedback Mode (CFB)



CFB Properties

- Chaining dependencies
 - Ciphertext block c_j depends on all preceding plaintext blocks.
- Error propagation
 - Bit error in one ciphertext block affects the next several blocks
- Error recovery
 - Can recover from bit errors after several blocks
 - Can resynchronize after loss of blocks.
- Secure against known plaintext attack (plaintext substitution)
- Less vulnerable to tampering with ciphertext - cipher C_i 's impact on m_{i+1} is subtle (through encryption function) and thus less predictable

Multiple Encryption

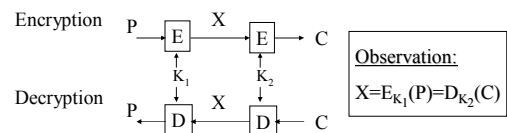
Multiple Encryption

- Major limitation of DES
 - Key length is too short (56 bits).
- Question: Can we apply DES multiple times to increase the strength of encryption?
 - Advantage: preserve the existing investment in software and equipment.

Multiple Encryption

- Double DES
 - Encrypt the plaintext twice with two different DES keys
 - Key length increases to 112 bits
- Two concerns
 - Is DES a group?
 - $E_{k_2}(E_{k_1}(P)) = E_{k_3}(P)$
 - Implication?
 - Meet-in-the-middle attack

Meet-in-the-middle attack

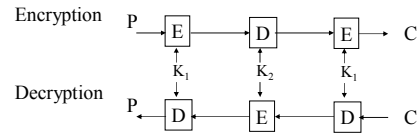


- Build table of 2^{56} 64-bit entries
 - Assume you have a few plaintext, ciphertext pairs $(p1, c1), (p2, c2), (p3, c3)$.
 - Encrypt P1 for all 2^{56} values for K_1 and store the results in a table.
 - Decrypt C1 for all 2^{56} values for K_2 , find expected 256 matches.
 - Then try those approximately 256 keys on 2nd plaintext, ciphertext pair
 - A successful decryption means the key is found.

Meet-in-the-middle attack Stats

- So time for bad guy isn't 2^{112}
- Instead it's 2 times 2^{56} DES operations or 2^{57}
- And memory is two times 2^{56} 64-bit words..

Triple DES



- Apply DES encryption/decryption three times.
 - With two keys or three keys
- Why E-D-E?
 - Initial and final permutations would cancel each other out with EEE (minor advantage to EDE)
 - EDE compatible with single DES if $K_1=K_2=K_3$.

Triple DES Is Not Ideal...

- Efficiency demands schemes with longer keys to begin with!
- Triple DES runs one third as fast as DES on the same platform
- New candidates are numerous - RC5, IDEA, two-fish, CAST, etc
- New AES