SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security and Resilience /
Advanced Security

Cryptography – Symmetric Key

Lecture Twenty

Lecture outline

- Symmetric key encryption
  - Stream ciphers
  - Block ciphers
  - DES
  - DES modes
  - Triple DES
  - AES
  - Other symmetric key encryption schemes

Learning goals

- By the end of this lecture the student should be able to
  - Explain the difference between a stream and block cipher
  - Outline the basic operation of the DES cipher algorithm
  - Explain the different DES modes
  - Explain 3DES
  - Explain AES

Symmetric cryptography

- Both sender and receiver use the same key for encryption and decryption
- Sometimes called 'secret key' cryptography
  - For encryption to be secure key needs to be kept secret
- Each pair of users who want to communicate must have two instances of the same key
  - Causes difficulties with key management
  - If 10 people in a group need to communicate then 45 keys needed
  - Total number of distinct keys needed is

$$\frac{n(n-1)}{2}$$

Types of symmetric systems

- Two types – Block Ciphers and Stream Ciphers
- Stream Ciphers
  - Attempt to emulate One-Time Pad Cipher
  - RC4 most widely implemented
- Block Ciphers
  - Encrypts blocks of n-bits of plaintext at once
  - DES most widely implemented

One time pad

- A perfect (unbreakable) encryption scheme if implemented properly
- Uses a pad made up of random values (binary)
  - The sender and receiver both have a copy of the pad
  - Once the pad is used it is destroyed
- Plaintext message translated into binary
- Plaintext is then XOR with the one time pad to produce the cipher text
- Receiver does another XOR on the cipher text to restore the plaintext
- Makes use of useful result that if

  `a` **`xor`** `b = c then c` **`xor`** `b = a`

One time pad

- `if a` **`xor`** `b = c then c` **`xor`** `b = a`

A	B	C (A xor B)	A (C xor B)
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

One time pad

Plain text message	1	0	0	1	0	0	1	0	0	1	1	0	1	0	0	1	1	0	1	1
One time pad	1	0	1	0	0	1	1	0	0	0	1	1	1	1	0	1	1	0	0	1
Cipher text	0	0	1	1	0	1	0	0	0	1	0	1	0	1	0	0	0	0	1	0

Cipher text	0	0	1	1	0	1	0	0	0	1	0	1	0	1	0	0	0	0	1	0
One time pad	1	0	1	0	0	1	1	0	0	0	1	1	1	1	0	1	1	0	0	1
Plain text message	1	0	0	1	0	0	1	0	0	1	1	0	1	0	0	1	1	0	1	1

One time pad

- The pad must be used once only
  - Reuse introduces patterns that might be exploited (in a frequency analysis for example)
- The pad must be as long as the message
  - To avoid reuse
- The pad must be securely distributed and protected at its destination
  - Most difficult aspect of one-time-pads or any secret key method of encryption

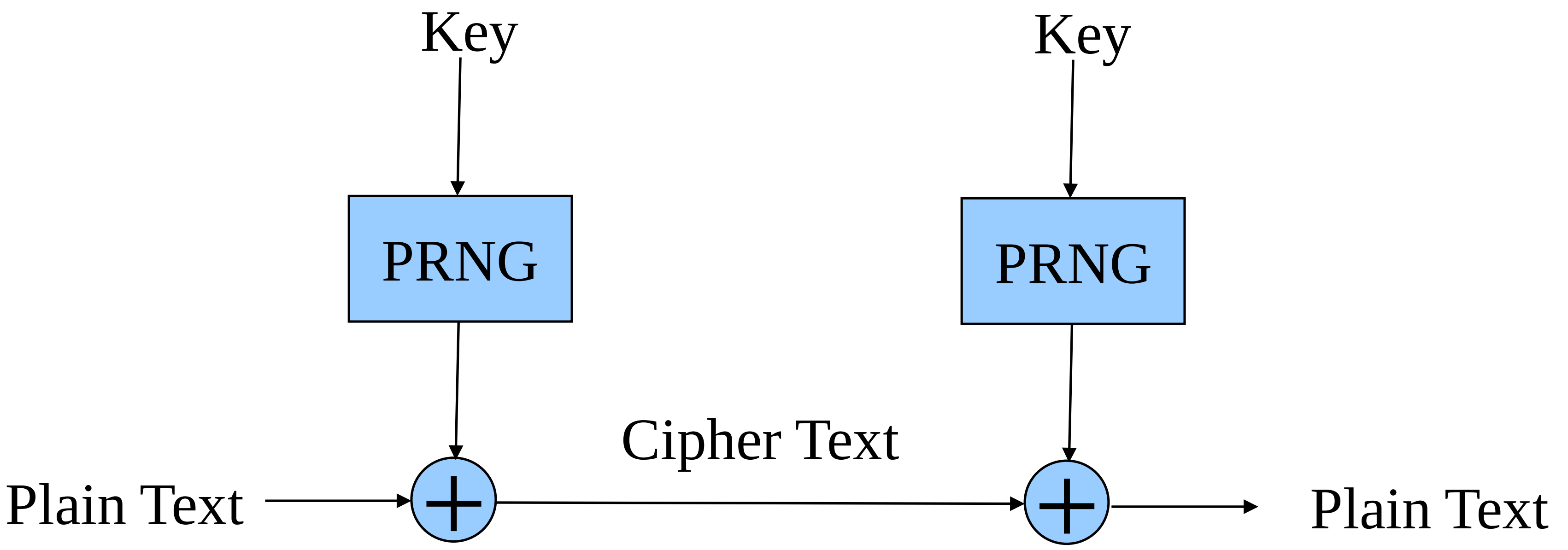
One time pad

- Pad must be made up of truly random values
  - If random values come from a pseudo random noise generator then knowledge of algorithm compromises one-time-pad
- Many cryptosystems attempt to emulate a one time pad
  - RC4
  - some DES modes (Cipher Feedback Mode, Output Feedback Mode, Counter Mode)

Stream ciphers

- A Stream Cipher is based on the 100% secure One-Time Pad Cipher that was discussed earlier.
- A Pseudo-Random bit generator is used rather than a purely random number source.
- The secret key is the seed for the pseudo-random generator
- Some stream ciphers are designed to produce one random bit at each cycle,
  - Easily implemented in hardware
- Software stream ciphers designs tend to produce a random byte or 32 bit word which is then XORed with the plaintext.

Stream ciphers



Question

- Using a stream cipher with the pseudo-random bit sequence 1 0 0 1 1 0 1 Encrypt and decrypt the following bit streams

  1 1 0 0 0 1 1

  0 0 0 0 1 1 1

Block cyphers

- Message divided into blocks of bits
- Processed a block at a time
- Made up of two processes
  - Confusion (substitution) and diffusion (transposition)
- The secret key governs which substitutions and transpositions are carried out

Substitution and transposition ciphers

- Symmetric keys built around substitution and transposition
- Substitution cipher
  - Based on a key
  - Substitute one value for another
- Transposition cipher
  - Based on a key
  - Move values from one position to another
- Most symmetric algorithms use multiple substitution and transpositions
  - Eg DES makes use of 16 rounds of substitution and transposition

Data Encryption Standard (DES)

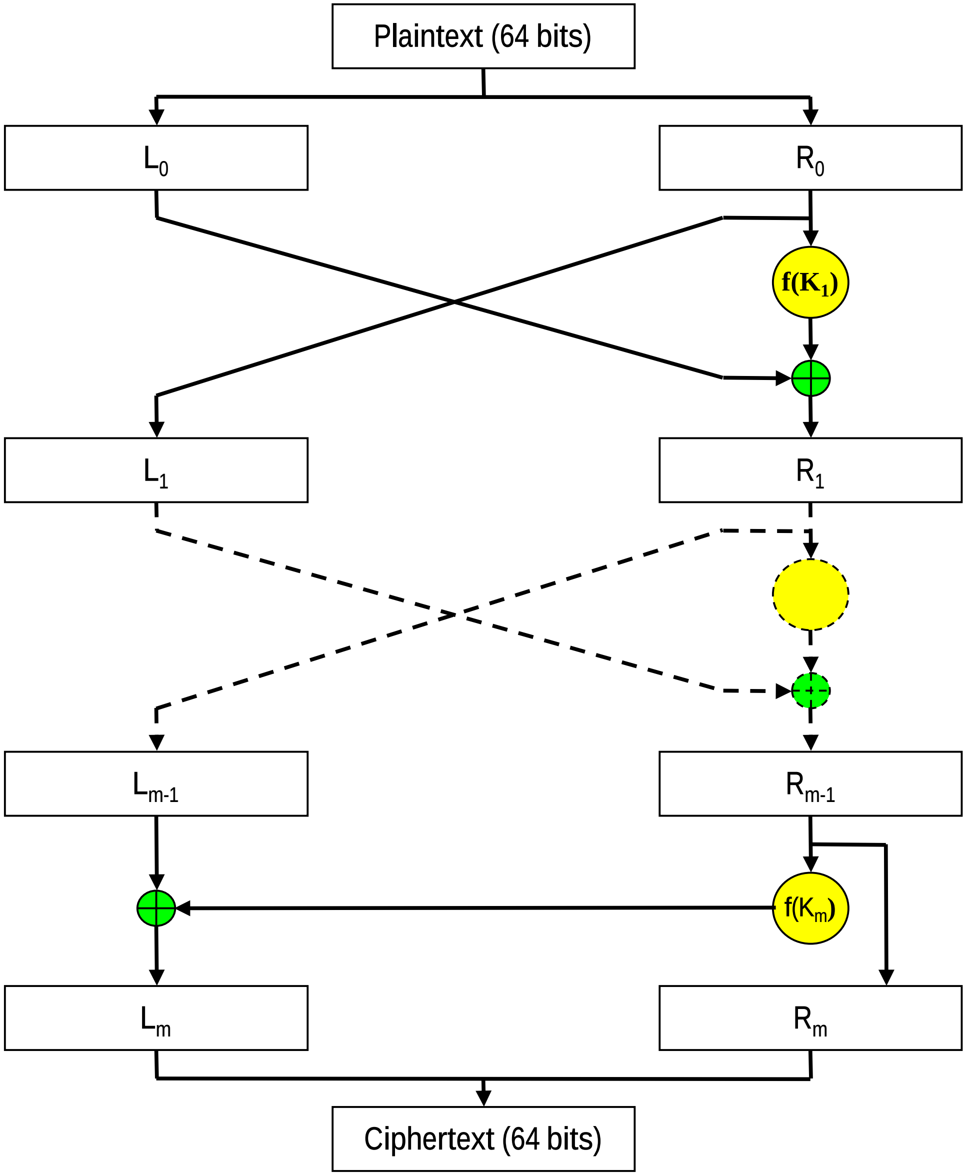
- Developed by IBM in response to a request by the US National Bureau of Standards for a government wide, unclassified encryption standard
- Proposed and published in 1975
- Some involvement of the National Security Agency (NSA)
  - Insisted on a shortened key length from 64 to 56 bits
    - Use 8 bits as Parity bits
  - Modified the S-Boxes (that carry out the substitutions in the algorithm)
- Approved as a standard in 1976

Data encryption standard

- DES is the most widely implemented encryption algorithm
  - A block cipher
  - Uses a network of ‘Feistel Functions’
- DES algorithm
  - Plaintext split into 64 bit blocks and produces 64 bit cipher text
  - Uses a 64 bit key
    - 56 bits for encryption, 8 bits for parity
  - 64 bit blocks are put through 16 rounds of transposition and substitution
  - The order and type of substitution depend on the value of the key
- DES makes use of one-way functions
  - Transpositions and XOR of key values
  - S-boxes

DES Algorithm

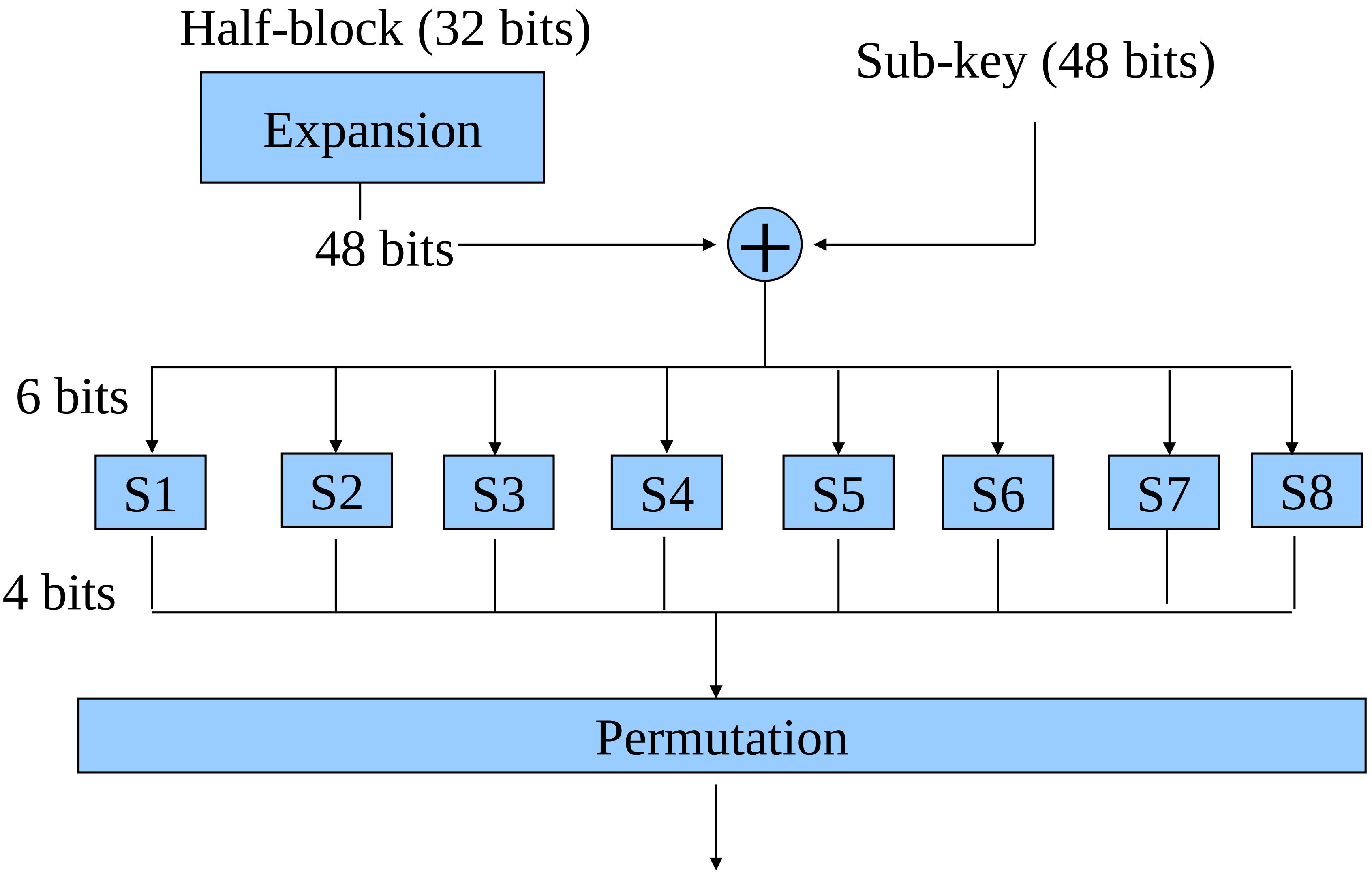
1. DES algorithm uses 16 stages
2. Each stage is split into a left and right half
3. The right half is used as input to a One-Way function (Feistel function) and its result is XORed with the left half, to form a new right half
4. The new left half is a simple copy of the original left half
5. This cycle is carried out 16 times
6. After the last cycle, the left and right halves are not exchanged
7. To decrypt we reverse the order of subkeys.



Feistel (F) function in DES

- *Expansion* — the 32-bit half-block is expanded to 48 bits by duplicating some of the bits.
- *Key mixing* — the result is combined with a *subkey* (derived from the shared key) using an XOR operation.
- *Substitution* — after key mixing, the block is divided into eight 6-bit pieces before processing by the S-Boxes. Each of the eight S-boxes replaces its six input bits with four output bits according to lookup table.
- *Permutation* — finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation (the *P-box*)

Feistel function



DES S-Box

- Takes a 6 bit input and substitutes it with a four bit output
- Eight S-Boxes – S1 to S8. S5 shown below
- an input "011011" has outer bits "01" and inner bits "1101"; the corresponding output would be "1001"

Middle 4 bits of input

S_5		**0000**	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
Outer bits	**01**	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Question

- What would be the output of S5 with an input of 110101?

DES Permutation

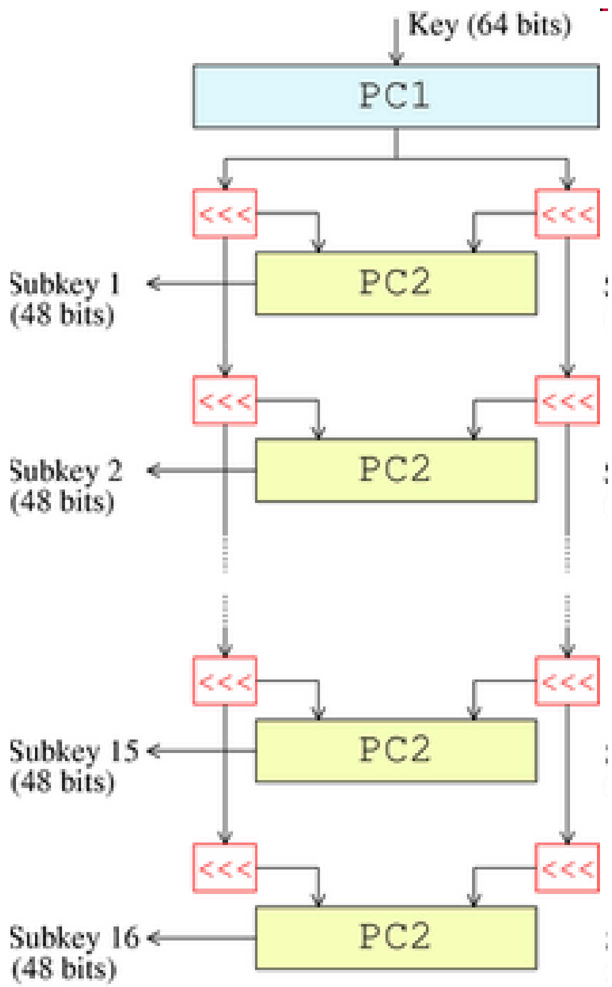
- A shuffling of the bits without modifying them
- DES Permutation P defined in the following table

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

- Using the above table, bit 16 in the input becomes bit 1, bit 7 become bit 2, bit 20 becomes bit 3…

DES Key schedule

- 48 bit sub-key is used in each Feistel function
- The sub-keys are generated through permutations in a similar way to P
- 64 bit key is input into PC1
- The 'parity' bits are removed from the key
- PC1 is a table defining a permutation of the 56 useful key bits
- PC2 defines 48 bit permutations of the key bits
- Decrypting DES uses exactly the same process as encryption, except that the subkeys are applied in reverse order

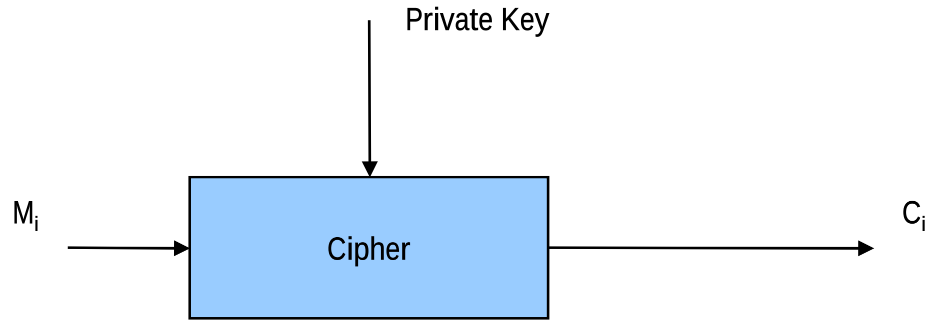


DES modes

- The basic mechanism of the 16 rounds of permutations and substitution provides a basic building block which can be used in different DES modes
- DES supports five modes
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter Mode (CM)

Electronic Code Book Mode

- Data is divided into 64-bit blocks and each block is encrypted one at a time.
  - Separate encryptions with different blocks are totally independent of each other.
  - This means that if data is transmitted over a network or phone line, transmission errors will only affect the block containing the error.
- Simplest mode of operation of a block cipher

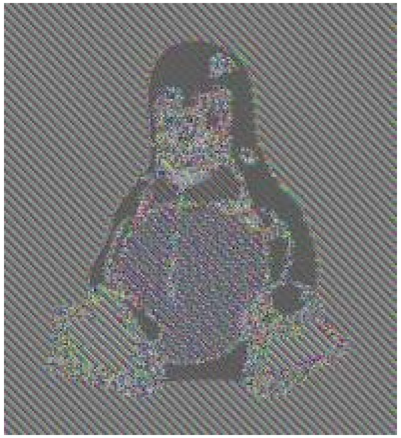


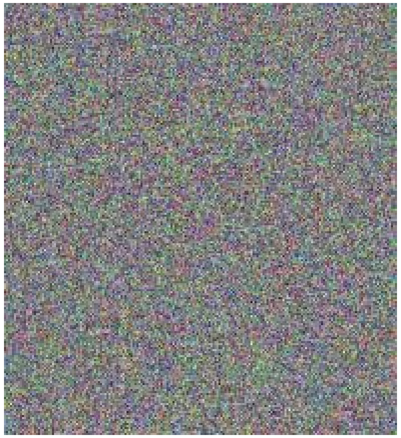
Electronic Code Book Mode

- Simplest and fast cryptosystem based on DES but least secure
- ECB mode results in each block being encrypted in the same way
  - Identical plaintexts will result in identical cipher texts
- ECB is the weakest of the various modes
  - No additional security measures are implemented besides the basic DES algorithm.
- Used for encrypting small amounts of data
  - PINs
- Should not be used for encrypting large amounts of data

Electronic code book encryption

- The following illustrates how ECB can leave plaintext patterns in the cypher text
- First picture is plain text, second is ECB cipher text, third is CBC cipher text
- (From Wikipedia)



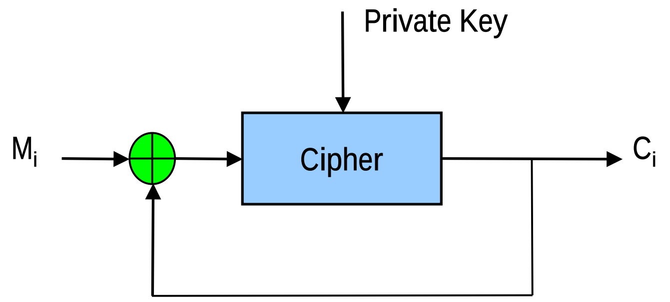


Cipher Block Chaining Mode

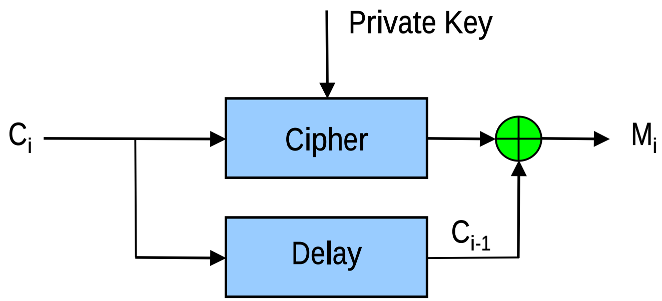
- Cipher Block Chaining (CBC) Mode adds a simple feedback mechanism to the cipher module.
  - Before a block of plaintext is encrypted, it is XORed with the previous block of ciphertext.
  - Can use a different block of text to start with as an initialisation vector
- At the receiving end, a block of ciphertext is decrypted and XORed with the previous block of unencrypted ciphertext to reproduce the plaintext.
  - Implemented by making a copy of the ciphertext block and delaying it a single cycle.
- This mode of operation gives much improved security
  - The same block of plaintext will not always encrypt to the same block of ciphertext
  - Consequently a hacker cannot slowly build up a codebook or easily decode common blocks.

Cipher Block Chaining Mode

Sender



Receiver



Initialisation Vector

- This technique also allows the system to generate different sequences for the same data set
- First time through the algorithm there is no “previous” value
  - By default the value will be zero
- By using a different starting value each time, a different sequence of cipher text values is generated
- The starting value is called the “Initialisation Vector”

Cipher Feedback Mode and Output Feedback Mode

- Emulates a one time pad
  - Suitable for streaming media
- Generates a (seemingly) random sequence of bits which are XORd with the plain text
  - Based on One Time Pad
- The same sequence is XORd with the cipher text at the receiver to recover the plaintext
- In order to produce a random series of bits, we need to feed a random selection of n-bit blocks to the cipher module.
- Cipher feedback mode, Output Feedback mode and Counter mode generate the random selection of bits
- Reverse process used for decryption

Attacking Symmetric Encryption

- Cryptanalysis is the science of breaking ciphers,
- Aim of cryptanalysis is, given ciphertext C, to recover either the plaintext P, the key K, or a weakness in the cipher that will eventually lead to the discovery of P or K.
- Cryptanalysis assumes no prior knowledge of the K, and always assume the cryptanalyst has access to the algorithm

Attacking Symmetric Encryption

- Attacks available to Cryptanalyst
  - Ciphertext Only – Access to encrypted messages only
  - Known Plaintext – And access to corresponding plaintext
  - Chosen Plaintext – And able to choose plaintext to be encrypted
  - Adaptive Chosen Plaintext – And able to reselect new plaintext after analysis
- Brute Force is variant on Ciphertext Only,
  - every key is tried until correct plaintext is found
- Goal of cryptanalysis is to find attacks that are faster than Brute Force

Attacking DES

- DES does have 64 weak keys which are easy to break
  - There is still another 72,057,594,037,927,872 keys
- Differential analysis was the approach that attracted most attention in DES attacks
  - Compares cipherblock pairs where plaintext pairs have a known difference
  - Assumes proximity in plaintext space leads to proximity in ciphertext space
  - Calculate probable keys after analysing many pairs
  - But does not work for DES

Attacking DES

- Brute Force Attack
  - Mathematically shown to be the best possible attack for DES
  - 16 rounds means that Differential Analysis no better (in fact slightly worse) than Brute force attack
    - 15 or less then Differential Analysis better
  - Increased CPU power means DES needs replacement
- Brute force attacks can be made highly parallel
- Brute force attacks highly scalable
  - Use 2 million chips then all keys checked in 6 minutes

Attacking DES

- DES Algorithm is very well understood
  - Subject to prolonged and sustained analysis
- It is known that the DES algorithm is ‘strong’
  - Brute force fastest method of attack
- But 56 bit key (56 secret bits + 8 bits ‘parity’) is too short
- Modern chipsets, 56 bit key can be decoded in an average time of 6 minutes, with a 2 million chip decoder
  - 64 bit key requires 1.07 days
  - 128 bit key more than 10^{16} years
- Interesting discussion on cracking DES
  - http://lasec.epfl.ch/memo/memo_des.shtml

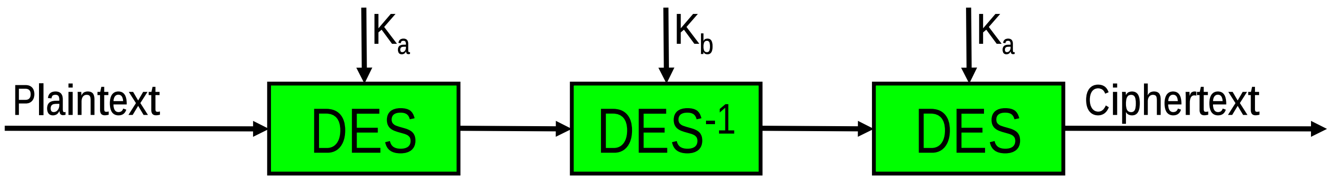
Key Lengths – Secretkey ciphers

Timeline	56 Bits	64 Bits	80 Bits	112 Bits	128 Bits
Now	6 minutes	1.07 days	191.7 years	8×10^{11} years	5×10^{16} years
Now + 5 years	36 s	2.6 hours	19.2 years	8×10^{10} years	5×10^{15} years
Now + 10 years	3.6 s	15.4 minutes	1.9 years	8×10^{9} years	5×10^{14} years
Now + 15 years	0.4 s	1.5 minutes	70 days	8×10^{8} years	5×10^{13} years
Now + 20 years	40 ms	9.2 s	7 days	8×10^{7} years	5×10^{12} years
Now + 25 years	4 ms	0.9 s	16.8 hours	8×10^{6} years	5×10^{11} years
Now + 30 years	0.4 ms	90 ms	1.7 hours	8×10^{5} years	5×10^{10} years
Now + 35 years	40 μs	9 ms	10 minutes	8×10^{4} years	5×10^{9} years
Now + 40 years	4 μs	0.9 ms	1 minute	8000 years	5×10^{8} years
Now + 45 years	0.4 μs	90 μs	6 seconds	800 years	5×10^{7} years

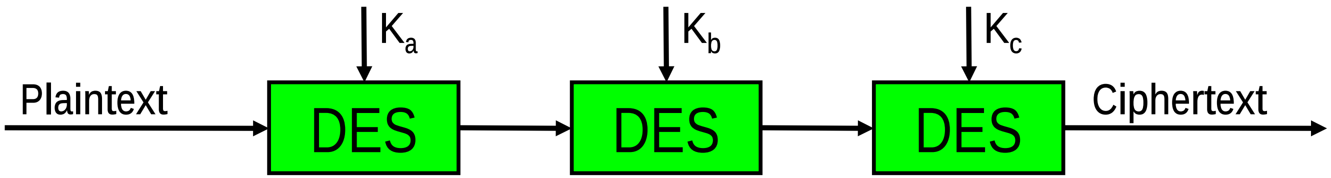
Assuming a computer that can try 2×10^{14} keys every second and Moore's Law doubling computer power every 18 months

Triple DES

- The biggest problem with DES is the size of the key – only 56 bits
  - In lieu of a standard with a larger key length, people have sought to modify DES to artificially increase its key length, the Result – Triple DES
  - Number of options. Most common is to use two 56 bit keys, Ka and Kb



  - Less commonly used is three keys



Triple DES

- Most common implementation of Triple-DES is a cipher with a 112 bit secret key
  - The key is divided into two 56 bit keys, K_a and K_b.
  - The plaintext is first encrypted using DES and K_a, the resultant ciphertext is then decrypted using DES and K_b
  - finally the intermediate plaintext is re-encrypted using K_a again.
  - The decryption process is the reverse.
  - This procedure has been shown to give security level equivalent to an 80 bit key
- Using three 56 bit keys gives security equivalent to a 112 bit key

Advanced Encryption Standard

- AES – Advanced Encryption Standard
  - DES replacement by NIST
  - Chosen through a competition
  - Developed in 1997
  - Symmetric block cipher
  - 128, 192, 256 bit keys
  - Able to run on variety of hardware
    - Smart cards, PDAs etc
    - Had to be computationally efficient
- AES is a subset of the Rijndael algorithm
  - Block Algorithm but without a Feistel Network
  - Number of rounds depends on key and block size
    - From 10 to 14

Advanced Encryption Standard

- The plain text is encrypted 128 bits at a time
- Each 128 bit block is structured as a 4 x 4 byte matrix
  - Input byte sequence is A00, A10, A20, A30, A01, A11, A21, A31,…
- Operations are carried out on this matrix
  - A number of rounds of substitution and permutation

A00	A01	A02	A03
A10	A11	A12	A13
A20	A21	A22	A23
A30	A31	A32	A33

Advanced Encryption Standard

- Depending on the key size different number of rounds are used
- Each round consists of
  - Substitution
  - ShiftRows: each row shifed cyclicly n – 1 bytes
  - MixColumns: each column multiplied by a fixed matrix (defined for each key length)
  - AddRoundKey: the 128 bit subkey is XORed with the matrix

Advanced Encryption Standard

S box and Mix columns matrix for 128 bit AES key length

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 7. S-box: substitution values for the byte xy (in hexadecimal format).

16

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

International Data Encryption Algorithm (IDEA)

- Similar to DES
- Longer key so much stronger than DES
  - 128 bits
- Faster than DES when implemented in software
- Used in PGP

RC4

- The most widely implemented stream cipher
- Invented by Ron Rivest of RSA
- Originally kept secret until source code published on a mailing list
- Used in WLAN (802.11) WEP security
- Used in WLAN 802.11i WPA security
- Very simple, fast and efficient, but with modern computing can be compromised quite quickly
  - Still widely used, but requires frequent key change (eg. WPA)

Blowfish, RC5 and RC6

- Blowfish
  - Block cipher
  - Keys up to 448 bits
  - 16 rounds of cryptographic functions
  - Designed by Bruce Schneier
- RC5
  - Block cipher developed by RSA
  - Main interesting thing is that block sizes can be 32, 64 or 128 bits
  - Key length is up to 2048 bits
- RC6
  - Developed for AES but not chosen
  - Some speed optimisations over RC5

Conclusion

- Symmetric key encryption
  - Stream ciphers
  - Block ciphers
  - DES
  - DES modes
  - Triple DES
  - AES
  - Other symmetric key encryption schemes