PART-1

Nguyễn Hồng Phước-51202890

Câu 1:

- S-DES Key Generation

10-bit key : 0111111101

Action	**Input**	**Output**
P10	0111111101	1111110011
LS-1	11111	11111
	10011	00111
P8	1111100111	01011111
		(K_1)
LS-2	11111	11111
	00111	11100
P8	1111111100	11111100
		(K_2)

- S-DES Encryption

8-bit plaintext : 10100010 (KC)

IP	10100010	00110001
E/P	0001	10000010
ExcusiveOR K_1	10000010,	11011101
S0	1101	11
S1	1101	00
P4	1100	1001
ExcusiveOR	1001, 0011	1010
SW	10100001	00011010
E/P	1010	01010101
ExcusiveORK_2	01010101,	10101001
S0	1010 10	
S1	1001 10	
P4	1010 0011	
ExcusiveOR	0001,0011	0010
IP^{-1}	00101010	00111000

8-bit ciphertext : 00111000

- S-DES Decryption

8-bit ciphertext : 00111000 (DH)

IP	00111000	00101010
E/P	1010	01010101
ExcusiveOR K_2	01010101,	10101001
S0	1010	10
S1	1001	10

P4	1010	0011
ExcusiveOR	0010,0011	0001
SW	00011010	10100001
E/P	0001	10000010
ExcusiveOR	K_1 10000010,	11011101
S0	1101	11
S1	1101	00
P4	1100	1001
ExcusiveOR	1010,1001	0011
IP^{-1}	00110001	10100010

8-bit plaintext : 10100010

Câu 2:

+) Ưu điểm của ECB.

- Đơn giản
- Không cần đồng bộ hóa giữa bên gửi và bên nhận.Nếu bên nhận không nhận đủ các khối, vẫn có thể giải mã các khối nhận được.
- Các bit lỗi sẽ không được đưa vào các khối kế sau
- Vì các khối được mã hóa và giải mã hoàn toàn độc lập với nhau nên ECB cho phép mã hóa và giải mã đồng thời nhiều khối(song song) nếu có đủ phần cứng để thực thi.

+) Nhược điểm của ECB

- ECB về bản chất giống hệt với mật mã bảng chữ cái cổ điển, chỉ có điều bảng chữ cái của ECB phức tạp hơn.
- Các khối bản rõ giống nhau sẽ được ánh xạ thành khối bản mã giống nhau(nếu dùng cùng 1 loại khóa) => dễ dàng tấn công bằng phương pháp thống kê tần suất
- ECB dễ dàng bị phá nếu plaintext lớn và có tính cấu trúc rõ ràng, từ đó ECB thường dùng để mã hóa những plaintext ngắn như khóa bí mật.
- ECB song song hóa được ,có cấu trúc(quy luật) => độ an toàn yếu) Chế độ CBC- Cipher Block Chaining (chế độ dây chuyền mã khối)
- Trong mô hình CBC, bản mã của một lần mã hóa được sử dụng cho lần mã hóa tiếp theo.
- Do đó để mã hóa khối đầu tiên, người ta dùng một khối dữ liệu giả được gọi là vector khởi tạo (initialization vector – IV) và được chọn ngẫu nhiên:
- Để giải mã, tiến hành ngược lại.
- Người mã hóa và người giải mã phải dùng chung vector khởi tạo IV. Vector khởi tạo không cần giữ bí mật nên thường được gắn vào trước bản mã trước khi truyền thông điệp

+) Ưu điểm CBC.

- Nội dung của bản mã Ci không chỉ phụ thuộc vào bản rõ Pi mà còn phụ thuộc vào tất cả các bản rõ đứng trước và IV. Do đó nếu có hai bản rõ giống nhau thì hai bản mã sẽ không giống nhau (do IV ngẫu nhiên). Điều này khắc phục được hạn chế của mô hình ECB, từ bản mã người phá mã không thể phát hiện ra những đặc tính thống kê của dữ liệu.

+) Nhược điểm của CBC

- Bản rõ Pi không chỉ phụ thuộc vào bản mã Ci mà còn phụ thuộc vào bản mã Ci-1 đứng trước. Do đó nếu xảy lỗi trên đường truyền, chỉ cần một bít bị hỏng thì dẫn đến không thể giải mã được bản mã đó và bản mã tiếp theo sau
- Các bít lỗi sẽ bị đưa vào các khối tiếp theo
- Không song song hóa được
- Sự thay đổi của bản tin ở đâu đó sẽ kéo theo sự thay đổi của mọi khối mã.
- Cần giá trị vecto ban đầu IV được biết trước bởi người gửi và người nhận. Tuy nhiên nếu IV được gửi công khai , kẻ tấn công có thể thay đổi bit đầu tiên và thay đổi cả IV để bù trừ.

+) Ưu điểm của OFB
- OFB không song song hóa được => không có cấu trúc => an toàn hơn CTR
- Về cơ bản OFB giống hệt với CFB.
- Cải tiến của OFB nhằm tránh việc phát triển lỗi từ một lỗi trong quá trình truyền.

+)Nhược điểm: Giống với CBC

+) Ưu điểm của CTR
- Hard effeciency : CTR cho phép mã và giải mã các khối một cách song song. CBC không thể thực hiện song song.
- Software effeciency: Do tận dụng được lợi thế xử lý song song nên CTR sẽ chạy nhanh hơn.
- Xử lý : Nếu bộ nhớ cho phép và vẫn đảm bảo được sự an toàn thì các output của khối mã hóa có thể được tính trước, từ đó mà tốc độ mã hóa sẽ rất nhanh.
- Cho phép truy nhập ngẫu nhiên các khối.

+) Nhược điểm của CTR
- Về tính an toàn CTR không mạnh như các chế độ khác.
- CTR có cài đặt tương đối đơn giản do mã và giải mã là như nhau
- CTR song song hóa được ,có cấu trúc(quy luật) => độ an toàn yếu
- CTR có cài đặt tương đối đơn giản.