NAME- RAM CHANDRA JANGIR
ROLL NO. - CS21M517
Subject - CS6530 - Assignment -1

FORMAT PRESERVING ENCRYPTION :-

(i) Introduction
(ii) Why we need FPE
(iii) Basic requirement for a viable FPE
(iv) Fiestel structure for FPE and details
(v) Credit card Encryption and Decryption
(vi) Running my program (ram_fpe) on ubuntu system

(i) Introduction :-

Format-preserving encryption (FPE) refers to any encryption technique that takes a plain text in a given format and produces a ciphertext in the same format.

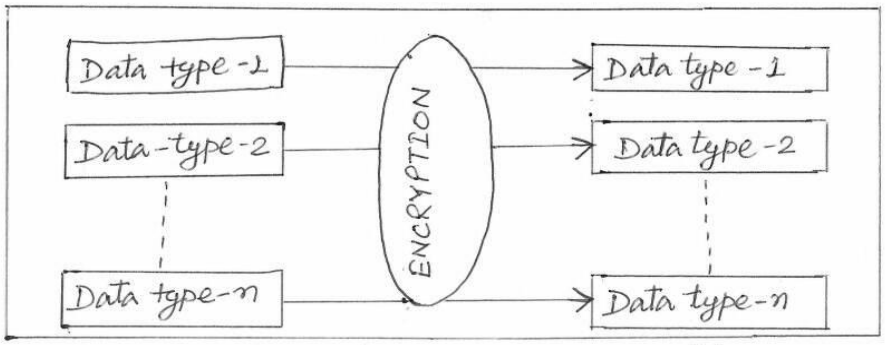

Figure - Format Preserving Encryption

The basic idea is using the symmetric key K, to encrypt a plain text into a cipher text B that has the same format as A.

(ii) Why we need FPE:-

During Encryption and Decryption, changing the database structure requires the lot of works. One of the main drawback of encryption methods is the cost of modifying databases and applications to store the encrypted information.
The main aim of FPE is to encrypt the data without changing the database structure, queries and all the applications programs that uses the data.

(iii) Basic requirements for a viable FPE technique:-

(a) The ciphertext is of the same length and format as the plaintext.
(b) It should be adaptable to work with a variety of character and number type.
(c) It should work with variable plaintext lengths.
(d) Security should be strong even for small plaintext lengths.

FPE algorithms implement "Fiestel structures", which are used to construct the block cipher. The structures are designed to convert any function (F-function) into a permutation.
Fiestel structures consists of rounds of reversible transformations consisting of three primary steps:

(a) splitting the data into two strings.
(b) Applying a keyed function to one of the strings
(c) Lastly reversing the roles of the strings for the subsequent rounds.

(iv) Fiestel structure for FPE:-

FPE can be implemented by Fiestel network. In Fiestel network, the subkeys are generated for each round. The keys are pseudo random values generated by AES algorithm.

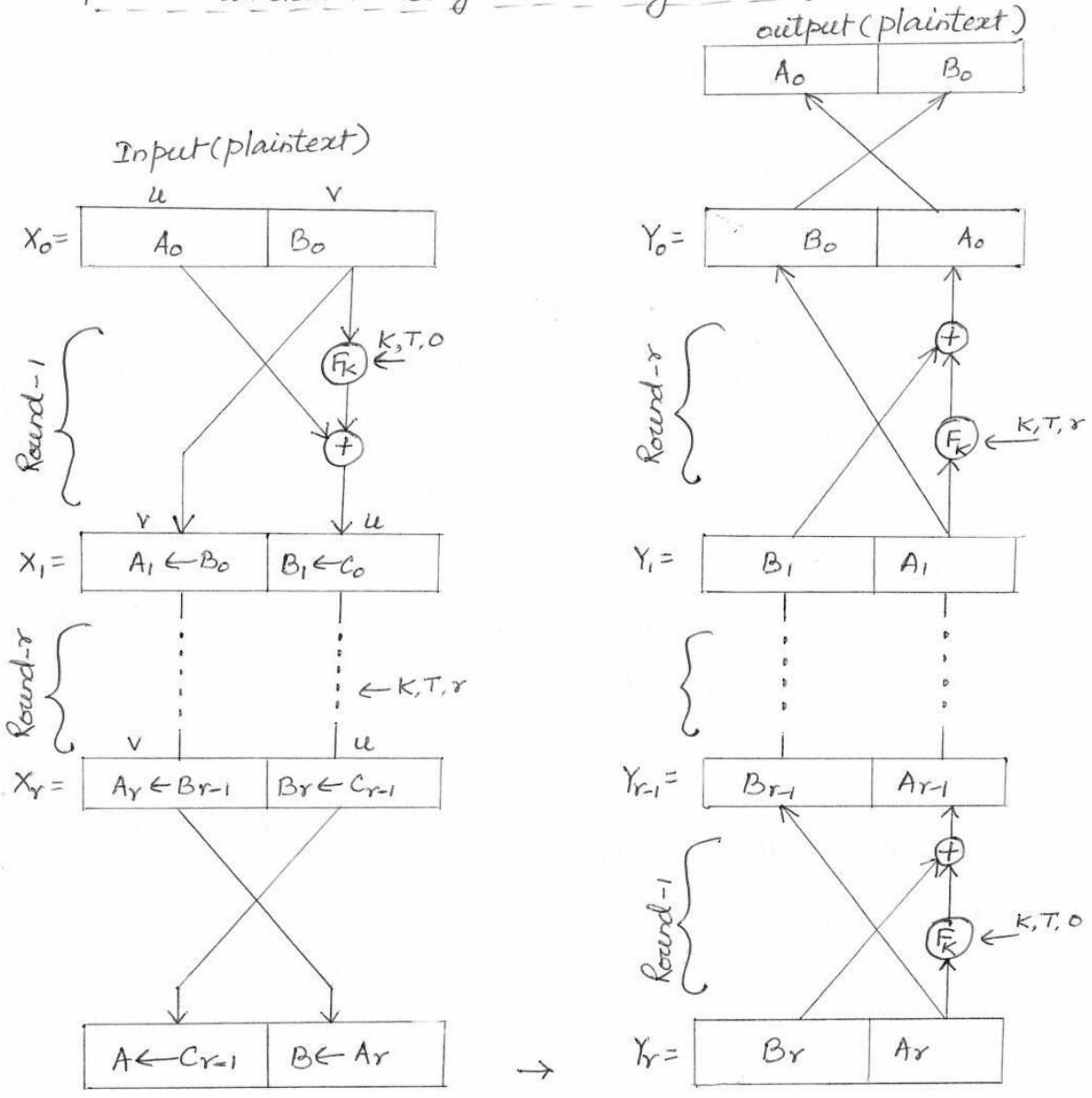

Figure-(i) Fiestel structure for FPE

Encryption and Decryption:

Figure-1 diagram shows the Fiestel structure used in FPE algorithms, with encryption shown on left-hand side and decryption on right hand side.

The input to the encryption algorithm is a plaintext character string of $n = u + v$ characters

$$u = \lfloor n/2 \rfloor$$
$$v = n - u$$

Each round i, has inputs A_r and B_r derived from preceding rounds. All rounds have same structure.

F_K is one way function, it has as parameters the secret key K, the plaintext length n, a tweak T and the round number r.

the process of decryption is same as the encryption process.

Character strings:

FPE algorithms are used with plaintext consisting of a string of elements, called characters.

The function F_K

The core of F_K is some type of randomizing function whose input and output are bit string.

Relationship between radix, message length and bit length;

consider a numeral string x of length len and base radix. if we convert this to a number x

$x = NUM_{radix}(X)$ then max. value of x is $(radix)^{len} - 1$.

The number of bits needed to encode x is

$$bitlen = \lceil \log_2(radix^{len}) \rceil = \lceil len \cdot \log_2(radix) \rceil$$

Observe that an increase in either radix or len increases bitlen.

(V) CREDIT CARD ENCRYPTION & DECRYPTION:

Here we plan to use a block cipher (AES algorithm) scheme for encrypting credit card number using format preserving encryption.

(i) Preparing plaintext for Encryption:

Consider 16-digit credit card Number (CCN).

The first six digits provide the issuer identification number (IIN), which identifies the institution, that issued the card.

The last ~~four digits~~

The remaining nine digits are the user's account number.

However a number of applications require that the last four digits be in the clear (the check digit plus three account digits) for applications such as credit card receipts, which leaves only six digits for encryption.

CCN	Tweak	Plaintext
4514 5600 0185 1363	4514561363	000185

For CCN encryption & decryption we are taking format-preserving encryption FF1 algorithm.

The internal functions of FF1 is based on AES-128 block cipher algorithm.

Algorithm	FF1	Structure
Block size (bits)	128	Fiestel
Number of rounds	10	
Key size	128	
CIPH function	AES-128	

FFX receives two of inputs

(a) X : a numeral string x of length n.

(b) T : a tweak of length t.

(c) radix : Number of elements in domains used in plaintext

(d) Y : Encrypted output (ciphertext)

(e) K : Key

Example

CCN	4514 5600 0185 1363	
Issuer Identification Number	4514 56	
T.I.N.	1363	
KEY	2b7e151628aed2a6abf7158809cf4f3c	K
Tweak	4514561363	T
Plaintext	000185	X
ciphertext	490035	Y
Encrypted CCN	4514564900351363	

- FFL has atleast 10 rounds of Fiestel. (more if message size or format is large.
- The round function is one invocation of AES.
- Thus atleast 10 calls to AES needed for each encryption or decryption.
- Below diagram and algorithm 1 represent two rounds and encryption function of FFL respectively.

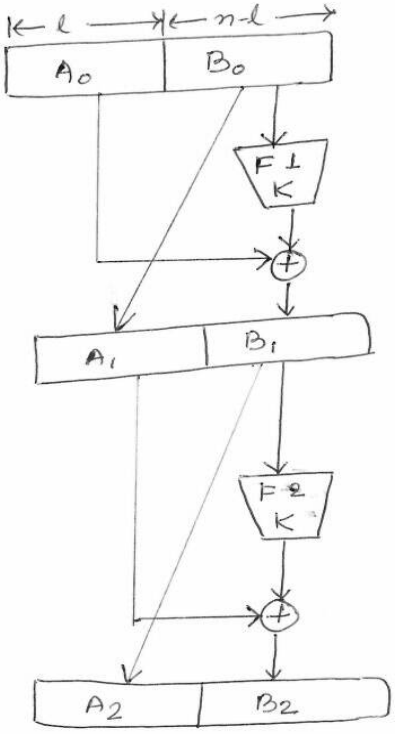

Figure - 2. Two Rounds of FFL

Algorithm 1: $FFL_K^{NT}(X)$

1. $(a,b) \leftarrow N$; $X_0 \leftarrow X$
2. for $i = 1, 2, \ldots, r(N)$ do
3. $A_{i-1} \leftarrow X_{i-1} \text{ div } b$
4. $B_{i-1} \leftarrow X_{i-1} \bmod b$
5. $C_i \leftarrow (A_{i-1} + F_K(N, T, i, B_{i-1})) \bmod a$
6. $X_i \leftarrow aB_{i-1} + C_i$
7. ret $X_{r(N)}$

vi) Example Output of My FPE program Built and Verified on Ubuntu System:

Program Name	ram_fpe
Key (Input)	2b7e151628aed2a6abf7158809cf4f3c
CCN	4514 5600 0185 1363

rjangir@rjangir-linux:/local/mnt/workspace/rjangir/WORKSPACE/ram_fpe$ ./ram_fpe
Usage: ./ram_fpe <key> <credit card number (16digits)>

rjangir@rjangir-linux:/local/mnt/workspace/rjangir/WORKSPACE/ram_fpe$ ./ram_fpe 2b7e151628aed2a6abf7158809cf4f3c 4514560001851363

##

Block Cipher Modes of Operation
Format-Preserving Encryption

##

FF1-Based on AES with Block Size as 128

Key is 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
Radix = 10

Credit Card Number is < 4 5 1 4 5 6 0 0 0 1 8 5 1 3 6 3>

Tweak is 45 14 56 13 63
Issuer Identification Number is 4 5 1 4 5 6 >

Transaction Identification Number is 1 3 6 3 >

Plaintext is < 0 0 0 1 8 5>

FF1_encrypt()

X is 0 0 0 1 8 5
Tweak is 45 14 56 13 63

Step 1:
u is 3, v is 3
Step 2:
A is 0 0 0

B is 1 8 5

Step 3:

b is 2

Step 4:

d is 8

Step 5:

P is [1 2 1 0 0 10 10 3 0 0 0 6 0 0 0 5]

Round #0

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 0 0 185]

Step 6.ii

R is [11 230 58 161 37 222 80 252 244 183 113 50 75 74 124 187]

Step 6.iii

S is be63aa125de50fc

Step 6.iv

y is BE63AA125DE50FC

Step 6.v

m is 3

Step 6.vi

c is 556

Step 6.vii

C is 5 5 6

Step 6.viii

A is 1 8 5

Step 6.ix

B is 5 5 6

Round #1

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 1 2 44]

Step 6.ii

R is [235 105 83 156 62 119 80 178 166 167 213 175 36 40 134 11]

Step 6.iii

S is eb69539c3e7750b2

Step 6.iv

y is EB69539C3E7750B2

Step 6.v

m is 3

Step 6.vi

c is 443

Step 6.vii

C is 4 4 3

Step 6.viii

A is 5 5 6

Step 6.ix

B is 4 4 3

Round #2

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 2 1 187]

Step 6.ii

R is [62 110 159 3 56 176 74 220 227 63 9 234 101 47 108 233]

Step 6.iii

S is 3e6e9f338b04adc

Step 6.iv

y is 3E6E9F0338B04ADC

Step 6.v

m is 3

Step 6.vi

c is 616

Step 6.vii

C is 6 1 6

Step 6.viii

A is 4 4 3

Step 6.ix

B is 6 1 6

Round #3

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 3 2 104]

Step 6.ii

R is [233 224 134 197 12 172 18 171 157 153 120 216 154 73 63 130]

Step 6.iii

S is e9e086c5cac12ab

Step 6.iv

y is E9E086C50CAC12AB

Step 6.v

m is 3

Step 6.vi

c is 334

Step 6.vii

C is 3 3 4

Step 6.viii

A is 6 1 6

Step 6.ix

B is 3 3 4

Round #4

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 4 1 78]

Step 6.ii

R is [113 195 29 11 54 131 5 176 38 107 220 31 83 67 130 195]

Step 6.iii

S is 71c31db36835b0

Step 6.iv

y is 71C31D0B368305B0

Step 6.v

m is 3

Step 6.vi

c is 400

Step 6.vii

C is 4 0 0

Step 6.viii

A is 3 3 4

Step 6.ix

B is 4 0 0

Round #5

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 5 1 144]

Step 6.ii

R is [236 10 100 80 2 121 158 82 50 111 165 38 31 221 195 222]

Step 6.iii

S is eca64502799e52

Step 6.iv

y is EC0A645002799E52

Step 6.v

m is 3

Step 6.vi

c is 888

Step 6.vii

C is 8 8 8

Step 6.viii

A is 4 0 0

Step 6.ix

B is 8 8 8

Round #6

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 6 3 120]

Step 6.ii

R is [227 166 60 152 255 121 14 149 114 154 26 19 233 128 20 0]

Step 6.iii

S is e3a63c98ff79e95

Step 6.iv

y is E3A63C98FF790E95

Step 6.v

m is 3

Step 6.vi

c is 989

Step 6.vii

C is 9 8 9

Step 6.viii

A is 8 8 8

Step 6.ix

B is 9 8 9

Round #7

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 7 3 221]

Step 6.ii

R is [87 203 49 160 27 165 129 27 227 152 8 54 7 172 0 51]

Step 6.iii

S is 57cb31a01ba5811b

Step 6.iv

y is 57CB31A01BA5811B

Step 6.v

m is 3

Step 6.vi

c is 195

Step 6.vii

C is 1 9 5

Step 6.viii

A is 9 8 9

Step 6.ix

B is 1 9 5

Round #8

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 8 0 195]

Step 6.ii

R is [231 127 114 173 57 223 9 157 160 207 245 135 101 68 23 218]

Step 6.iii

S is e77f72ad39df99d

Step 6.iv

y is E77F72AD39DF099D

Step 6.v

m is 3

Step 6.vi

c is 490

Step 6.vii

C is 4 9 0

Step 6.viii

A is 1 9 5

Step 6.ix

B is 4 9 0

Round #9

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 9 1 234]

Step 6.ii

R is [48 187 21 199 245 250 39 136 251 105 127 144 246 5 100 218]

Step 6.iii

S is 30bb15c7f5fa2788

Step 6.iv

y is 30BB15C7F5FA2788

Step 6.v

m is 3

Step 6.vi

c is 035

Step 6.vii

C is 0 3 5

Step 6.viii

A is 4 9 0

Step 6.ix

B is 0 3 5

Step 7

CIPHERTEXT (A||B) is 4 9 0 0 3 5

ciphertext: 490035

****

ciphertext: 490035

Encrypted Credit Card Number : 4 5 1 4 5 6 4 9 0 0 3 5 1 3 6 3

****

We start Decrypting the cipher back

FF1_decrypt()

X is 4 9 0 0 3 5
Tweak is 45 14 56 13 63

Step 1:
u is 3, v is 3
Step 2:
A is 4 9 0
B is 0 3 5
Step 3:
b is 2
Step 4:
d is 8
Step 5:
P is [1 2 1 0 0 10 10 3 0 0 0 6 0 0 0 5]

Round #9
Step 6.i
Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 9 1 234]
Step 6.ii
R is [48 187 21 199 245 250 39 136 251 105 127 144 246 5 100 218]
Step 6.iii
S is 30bb15c7f5fa2788
Step 6.iv
y is 30BB15C7F5FA2788
Step 6.v
m is 3
Step 6.vi
c is 490
Step 6.vii
C is 4 9 0
Step 6.viii
A is 1 9 5
Step 6.ix
B is 4 9 0

Round #8
Step 6.i
Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 8 0 195]
Step 6.ii

R is [231 127 114 173 57 223 9 157 160 207 245 135 101 68 23 218]

Step 6.iii

S is e77f72ad39df99d

Step 6.iv

y is E77F72AD39DF099D

Step 6.v

m is 3

Step 6.vi

c is 195

Step 6.vii

C is 1 9 5

Step 6.viii

A is 9 8 9

Step 6.ix

B is 1 9 5

Round #7

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 7 3 221]

Step 6.ii

R is [87 203 49 160 27 165 129 27 227 152 8 54 7 172 0 51]

Step 6.iii

S is 57cb31a01ba5811b

Step 6.iv

y is 57CB31A01BA5811B

Step 6.v

m is 3

Step 6.vi

c is 989

Step 6.vii

C is 9 8 9

Step 6.viii

A is 8 8 8

Step 6.ix

B is 9 8 9

Round #6

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 6 3 120]

Step 6.ii

R is [227 166 60 152 255 121 14 149 114 154 26 19 233 128 20 0]

Step 6.iii

S is e3a63c98ff79e95

Step 6.iv

y is E3A63C98FF790E95

Step 6.v

m is 3

Step 6.vi

c is 888

Step 6.vii

C is 8 8 8

Step 6.viii

A is 4 0 0

Step 6.ix

B is 8 8 8

Round #5

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 5 1 144]

Step 6.ii

R is [236 10 100 80 2 121 158 82 50 111 165 38 31 221 195 222]

Step 6.iii

S is eca64502799e52

Step 6.iv

y is EC0A645002799E52

Step 6.v

m is 3

Step 6.vi

c is 400

Step 6.vii

C is 4 0 0

Step 6.viii

A is 3 3 4

Step 6.ix

B is 4 0 0

Round #4

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 4 1 78]

Step 6.ii

R is [113 195 29 11 54 131 5 176 38 107 220 31 83 67 130 195]

Step 6.iii

S is 71c31db36835b0

Step 6.iv

y is 71C31D0B368305B0

Step 6.v

m is 3

Step 6.vi

c is 334

Step 6.vii

C is 3 3 4

Step 6.viii

A is 6 1 6

Step 6.ix

B is 3 3 4

Round #3

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 3 2 104]

Step 6.ii

R is [233 224 134 197 12 172 18 171 157 153 120 216 154 73 63 130]

Step 6.iii

S is e9e086c5cac12ab

Step 6.iv

y is E9E086C50CAC12AB

Step 6.v

m is 3

Step 6.vi

c is 616

Step 6.vii

C is 6 1 6

Step 6.viii

A is 4 4 3

Step 6.ix

B is 6 1 6

Round #2

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 2 1 187]

Step 6.ii

R is [62 110 159 3 56 176 74 220 227 63 9 234 101 47 108 233]

Step 6.iii

S is 3e6e9f338b04adc

Step 6.iv

y is 3E6E9F0338B04ADC

Step 6.v

m is 3

Step 6.vi

c is 443

Step 6.vii

C is 4 4 3

Step 6.viii

A is 5 5 6

Step 6.ix

B is 4 4 3

Round #1

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 1 2 44]

Step 6.ii

R is [235 105 83 156 62 119 80 178 166 167 213 175 36 40 134 11]

Step 6.iii

S is eb69539c3e7750b2

Step 6.iv

y is EB69539C3E7750B2

Step 6.v

m is 3

Step 6.vi

c is 556

Step 6.vii

C is 5 5 6

Step 6.viii

A is 1 8 5

Step 6.ix

B is 5 5 6

Round #0

Step 6.i

Q is [69 20 86 19 99 0 0 0 0 0 0 0 0 0 0 185]

Step 6.ii

R is [11 230 58 161 37 222 80 252 244 183 113 50 75 74 124 187]

Step 6.iii

S is be63aa125de50fc

Step 6.iv

y is BE63AA125DE50FC

Step 6.v

m is 3

Step 6.vi

c is 185

Step 6.vii

C is 1 8 5

Step 6.viii

A is 0 0 0

Step 6.ix

B is 1 8 5

Decrypted Card Number

Plaintext: < 4 5 1 4 5 6 0 0 0 1 8 5 1 3 6 3 >

rjangir@rjangir-linux:/local/mnt/workspace/rjangir/WORKSPACE/ram_fpe$