On adaptive of classical and public key cryptography by using $\mathcal{E}$-$\mathcal{A}$ and $\mathcal{D}$-$\mathcal{A}$ laws

AMEER A.J. AL-SWIDI
University of Babylon ,Collage of Education for pure sciences,
Math. Department.
Waleedabd73@yahoo.com

Abstract:

In this paper I give a new definition $\mathcal{E}$-$\mathcal{A}$ and $\mathcal{D}$-$\mathcal{A}$ which is used to encipher and decipher which give more authentication and complexity for cryptography,and I use my definition in some type of classical and public key cryptography.

Key word: P , C,k, $\mathcal{E}$-$\mathcal{A}$, $\mathcal{D}$-$\mathcal{A}$, min ,max,r,q,e,d,n.

1.Introduction:

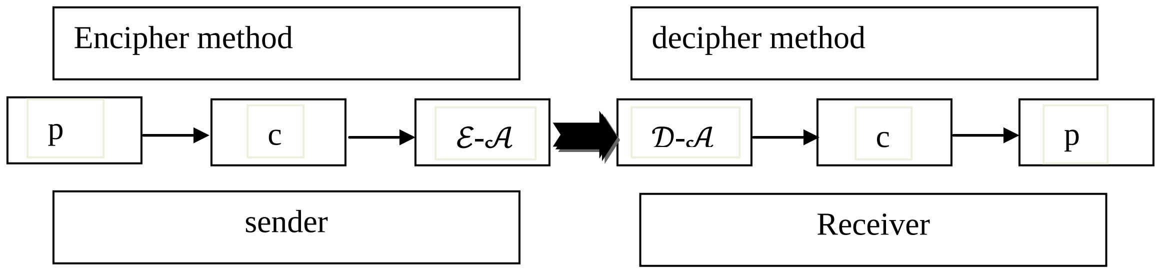
Simple substitution cipher are generally easy to break in aciphertext –only attack using single –letter frequency distribution (cf.[3,6,7,11]) ,cipher based on shifted alphabets are usually easy to solve ,because each ciphertext letter is a constant distant from its corresponding plaintext letter .because simple substitution cipher use a single mapping from plaintext to ciphertext letter ,the single-letter frequency distribution of the plaintext letter is preserved in the ciphertext .homophonic substitutions conceal this distribution by defining multiple ciphertext elements for each plaintext letter .polyalphabetic substitution cipher conceal it by using multiple substitutions.the development of polyalphabetic cipher began with Leon Battista Alberti, in 1568 Alberti puplished a manuscript describing a cipher disk that defined multiple substitutions, most polyalphabetic ciphers are periodic substitution ciphers based on aperiod d,given d cipher alphabets $c_1,c_2,\ldots\ldots,c_d$ let $f_i:p\rightarrow c_i$ be a mapping from the plaintext alphabets p to the ith cipher alphabet c_i $(1\leq i\leq d)$,For the special case d=1, the cipher is monoalphabetic and equivalent to simple substitution ,now for vigenere ,Beaufort ,Variant Beaufort and Hill ciphers(cf.[2,8,11]),

And in 1978,Pohlig and Hellman published an encryption scheme based on computing exponentials over a finite field,at about the same time ,Rivest,Shamir,and Adleman published a similar scheme,the encipher and decipher transformation are based on Euler's generalization of Fermat's Theorem ,which states that for every p relatively prime to k(n) ,(cf.[1,4,5,9,10,12]), for digital signature in classical and public key cryptography by using $\mathcal{E}$-$\mathcal{A}$ and $\mathcal{D}$-$\mathcal{A}$ laws, I use the laws $\mathcal{E}$-$\mathcal{A}$ and $\mathcal{D}$-$\mathcal{A}$ where

$\mathcal{E}$-$\mathcal{A}$=min(max(26-c,k),max(c,26-k))

$\mathcal{D}$-$\mathcal{A}$=min(max(26- $\mathcal{E}$-$\mathcal{A}$,k),max($\mathcal{E}$-$\mathcal{A}$,26-k))

And this figure which show as the encipher and decipher ,



Fiq(1)

Where p-represented the plainte[illegible]iphertext ,min- represented the minimum values ,max-represented the maximum values and 26-number of alphabets .

Key word mixed alphabets

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2.Some classical cryptography:

<u>2.1.vigenere cipher:</u>

A popular form of periodic substitution cipher based on shifted alphabets is the vigenere cipher,this cipher has been attributed to the 16^{th} century French cryptologist Blaise de vegenere .(cf.[2,6,11])

The encipher is

C=(p+k) mod 26

The decipher is

P=(c-k)mod26

2.2.Example:

Let the plaintext (p=7≡h) and(k=35) secrete key So, to encipher

C=(p+k)mod26

=(7+35)mod26

=16≡q

To decipher is

P=(c-k)mod26

=(16-35)mod26

=7≡h

2.3.Beaufort cipher :

The Beaufort cipher is similar,using the substitution

C=(k-p)mod26

Note that the same function can be used to decipher ,that is,for ciphertext letter c,

P=(k-p)mod26

The Beaufort cipher reverses the letters in the alphabet,and then shifts them to the right by(k+1) positions,this can be seen by rewriting p as follows:

C=[(26-1)-p+(k+1)]mod26…….(cf.[2,6,11])

2.4.Example:

Let the plaintext (p=7≡h) and(k=35) secrete key So, to encipher

C=(k-p) mod26

=(35-7)mod26
=2≡c
To decipher is
P=(k-p)mod26
= (35-2) mod26
=7≡h

2.5.variant Beaufort cipher :
The variant Beaufort cipher is equivalent to a vigenere cipher with key character (26-k),the variant Beaufort cipher is also the inverse of the vigenere cipher(cf.[2,6,11]),and its uses the substitution
C=(p-k)mod26
And to decipher
P=(c+k)mod26
2.6.Example:
Let the plaintext (p=7≡h) and(k=35) secrete key So, to encipher
C=(p-k) mod26
=(7-35)mod26
=24≡y
To decipher is
P=(c+k)mod26
= (24+35) mod26
=7≡h
2.7.Hill cipher :
The Hill cipher performs a linear transformation on plaintext characters to get ciphertext characters, the encipher is uses(cf.[6,7,11])
$C=E_k(p)=(p*k)mod26$
Decipher is done using the inverse key k^{-1} ,
$D_K=k^{-1}*c$ mod26
$=k^{-1}*k*p$ ood26
=p
2.8.Example:
Let the plaintext (p=5≡F) , ($k=61,k^{-1}=3$) secrete key So, to encipher
C=(p*k) mod26
=(5*61)mod26
=19≡T
To decipher is
$P=c*k^{-1}$ mod26
= (19*3) mod26
=5≡F
3.Some public key- cryptography:
3.1.Pohlig-Hellman cipher:
In the Pohlig-Hellman scheme, the modulus is chosen to be a large prime K,the enciphering functions are thus given by:
$C=p^e$ mod k
and deciphering functions are thus given by:
$p=c^d$ mod k

where all arithmetic is done in the GF(k)(cf.[3,4,10]),because k-prime , Ø(k)=k-1,thus the scheme can only be used for conventional encryption,where e and d are both kept secret.

3.2.example:

Let the plaintext (p=8≡I) , (k=29) secrete key So, to encipher

_ First we compute e-kept secret by

$e=d^{\emptyset(\emptyset(k))-1} \bmod \emptyset(k)$

$=3^{\emptyset(28)-1} \bmod 28$

$=3^{11} \bmod 28$

$=19$

Now encipher

$C=p^{e} \bmod k$

$=8^{19} \bmod 29$

$=2\equiv C$

To decipher is

$p=c^{d} \bmod k$

$=2^{3} \bmod 29$

$=8\equiv I$

3.3. Rivest-Shamir-Adleman(RSA) cipher:

In the RSA scheme,the modulus n is the product of two large primes r and q:

n=rq

thus

Ø(n)=(r-1)(q-1)

the enciphering functions are thus given by:

$C=p^{e} \bmod n$

and deciphering functions are thus given by:

$p=c^{d} \bmod n$

Rivest-Shamir and Adleman recommend picking d relatively prime to Ø(n) in the interval [max(r,q)+1,n-1],and compute e(cf.[3,4,10])

3.4.Example:

Let the plaintext (p=8≡I) , (r=5,q=7,d=7) secrete key So, n=rq=5*7=35 to encipher

_ First we compute e-kept secret by

$e=d^{\emptyset(\emptyset(n)-1} \bmod \emptyset(n)$

$=7^{\emptyset(24)-1} \bmod 24$

$=7^{\emptyset((2^{3})*3)-1} \bmod 24$

$=7^{7} \bmod 24$

$=7$

Now encipher

$C=p^{e} \bmod n$

$=8^{7} \bmod 35$

$=22\equiv W$

To decipher is

$p=c^{d} \bmod k$

$=22^{7} \bmod 35$

$=8\equiv I$

4. digital signature in classical cryptography by using $\mathcal{E}$-$\mathcal{A}$ and $\mathcal{D}$-$\mathcal{A}$ laws:

4.1.$\mathcal{A}$-vigenere cipher:

The stongly of $\mathcal{A}$-vigenere cipher is by choosing k-large number,its means that by choosing k>26, where k-secrete key the laws which is used to encipher is,

C=(p+k)mod26

$\mathcal{E}$-$\mathcal{A}$=max(min(26-c,k),min(c,26-k))

And for decipher is,

$\mathcal{D}$-$\mathcal{A}$=max(min(26- $\mathcal{E}$-$\mathcal{A}$,k),min($\mathcal{E}$-$\mathcal{A}$,26-k))

P=($\mathcal{D}$-$\mathcal{A}$-k)mod26

4.2.Example:

Let the plaintext (p=7≡h) and(k=35) secrete key So, to encipher

C=(p+k)mod26
=(7+35)mod26
=16≡q

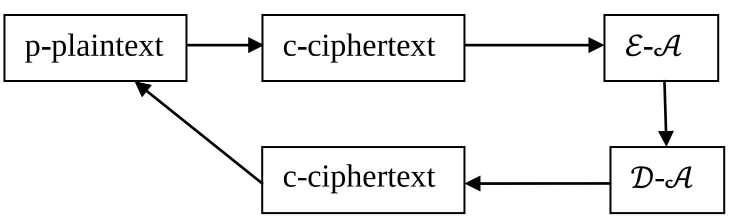
$\mathcal{E}$-$\mathcal{A}$=max(min(26-c,k),min(c,26-k))
=max(min(26-16,35),min(16,26-35))
=max(10,-19)
=10≡k

So that the plaintext is h and encipher to character q and by using $\mathcal{E}$-$\mathcal{A}$-law sender is k ,so that I give more authentication by using $\mathcal{E}$-$\mathcal{A}$-law,

Now to decipher, its means to repeats the plaintext is

$\mathcal{D}$-$\mathcal{A}$=max(min(26- $\mathcal{E}$-$\mathcal{A}$,k),min($\mathcal{E}$-$\mathcal{A}$,26-k))
=max(min(26- 10,35),min(10,26-35))
=max(16,-9)
=16≡q

P=($\mathcal{D}$-$\mathcal{A}$-k)mod26
=(16-35)mod26
=7≡h

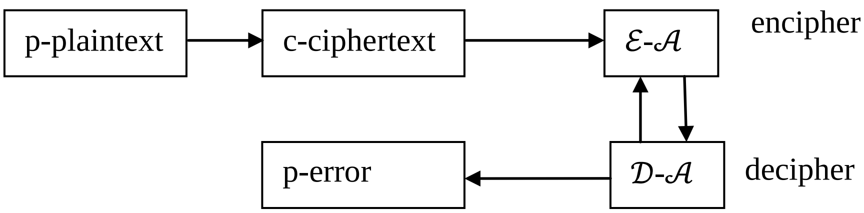


Fiq(2)

4.3.Remarks:

1- In the situation if k<p the $\mathcal{E}$-$\mathcal{A}$ and $\mathcal{D}$-$\mathcal{A}$ give the same value(characters)and decipher not give the correct p-plaintext its mean the method not work ,now for example if we take p=24≡y ,k=7,then

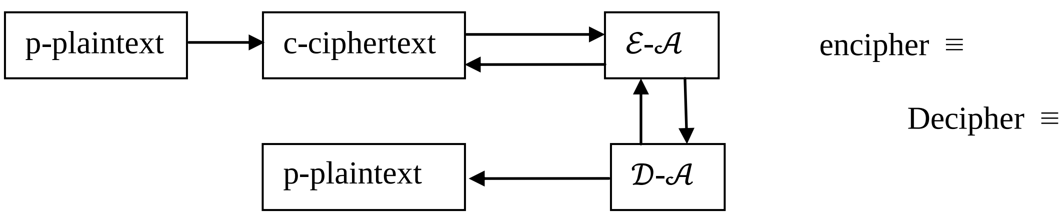
C=5 , $\mathcal{E}$-$\mathcal{A}$=**7** , $\mathcal{D}$-$\mathcal{A}$=**7** ,p=0≡A ≠ p=24≡y.



Fiq(3)

2- In the situation if k=p the c-ciphertext, ℰ -𝒜 and 𝒟-𝒜 give the same value(characters) its mean the ℰ -𝒜 and 𝒟-𝒜 laws not work, now for example if we take p=7≡H, k=7 then

C=**14** , ℰ -𝒜=**14** , 𝒟-𝒜=**14** ,p=7≡H



Fiq(4)

4.4.□-Beaufort cipher :

In this method its take similar substitution
C=(k-p)mod26
ℰ -□=max(min(26-c,k),min(c,26-k))
Note that the same function can be used to decipher ,that is for ciphertext letter c
□-□=max(min(26- ℰ -□,k),min(ℰ -□,26-k))
p=(k- □-□)mod26
4.5.Example:
Let the plaintext (p=7≡h) and(k=35) secrete key So, to encipher
C=(k-p) mod26
=(35-7)mod26
=2≡c
ℰ -□=max(min(26-c,k),min(c,26-k))
= max(min(26-2,35),min(2,26-35))
=max(24,- 9)
=24≡y
So that the plaintext is h and encipher to character c and by using ℰ -□-law sender is y ,so that I give more authentication by using ℰ -□-law,
Now to decipher, its means to repeats the plaintext is

□-□=max(min(26- ℰ -□,k),min(ℰ -□,26-k))
=max(min(26- 24,35),min(24,26-35))
=max(2,-9)
=2≡c
p=(k- □-□) mod26
= (35-2) mod26
=7≡h
The □-Beaufort cipher steps for encipher and decipher (see Fiq(2))

4.6.Remarks:

1- In the situation if k<p the c-ciphertext , ℰ -□ and □-□ give the same value(characters) its mean the ℰ -□ and □-□ laws not work, now for example if we take p=24≡y ,k=7,then
C=**9** , ℰ -□=**9** , □-□=**9**,p=24≡y…….(see Fiq(4))

2- In the situation if k=p the ℰ -□ and □-□ give the same value(characters)and decipher not give the correct p-plaintext its mean the method not work ,now for example if we take p=7≡H, k=7 then
p=7≡H ….(see Fiq(3))
C=0 , ℰ -□=**7** , □-□=**7** ,p=0≡A ≠

4.7.□- variant Beaufort cipher :

Uses the substitution
c=(p-k) mod26
ℰ -□=max(min(26-c,k),min(c,26-k))
And for decipher is,
□-□=max(min(26- ℰ -□,k),min(ℰ -□,26-k))
P=(□-□+k)mod26
Because
(p-k) mod26 ≡ (p+(26-k)) mod26

The □- variant Beaufort cipher is equivalent to a □-vigenere cipher with key character (26-k), the □-variant Beaufort cipher is also the inverse of the □-vigenere cipher, thus if one used to encipher, the other is used to decipher.

4.8.Example:

Let the plaintext (p=7≡h) and(k=35) secrete key So, to encipher
C=(p-k) mod26
=(7-35)mod26
=24≡y
ℰ -□=max(min(26-c,k),min(c,26-k))
= max(min(26-24,35),min(24,26-35))
=max(2,-9)
=2≡c

So that the plaintext is h and encipher to character y and by using ℰ -□-law sender is c ,so that I give more authentication by using ℰ -□-law,
Now to decipher, its means to repeats the plaintext is
□-□=max(min(26- ℰ -□,k),min(ℰ -□,26-k))
=max(min(26- 2,35),min(2,26-35))
=max(24,-9)
=24≡y

p=(□-□+k) mod26
= (24+35) mod26
=7≡h
The □- variant Beaufort cipher steps for encipher and decipher (see Fiq(2))

4.9.Remarks:

1- In the situation if k<p the c-ciphertext , ℰ -□ and □-□ give the same value(characters) its mean the ℰ -□ and □-□ laws not work, now for example if we take p=24≡y ,k=7,then
C=**17** , ℰ -□=**17**, □-□=**17**, p=24≡y…….(see Fiq(4))

2- In the situation if k=p the ℰ -□ and □-□ give the same value(characters)and decipher not give the correct p-plaintext its mean the method not work ,now for example if we take p=7≡H, k=7 then
p=7≡H ….(see Fiq(3))
C=0 , ℰ -□=**7** , □-□=**7** ,p=14≡O ≠

4.10.□- Hill cipher :

The □- **Hill cipher** performs a linear transformation on plaintext characters to get ciphertext characters, now encipher as
C=E_k(P)=(pk)mod26
ℰ -□=max(min(26-c,k),min(c,26-k))
And for decipher
□-□=max(min(26- ℰ -□,k),min(ℰ -□,26-k))
P=D_k(□-□)=(□-□*k^{-1})mod26
to compute inverse of k-secrete key, k*k^{-1}mod26=1 (cf.[00000])

4.11.Example:

Let the plaintext (p=5≡F) ,(k=61,k^{-1}=3) secrete key So, to encipher
C=(p*k) mod26
=(5*61)mod26
=19≡T

ℰ -□=max(min(26-c,k),min(c,26-k))
= max(min(26-19,61),min(19,26-61))
=max(7,-35)
=7≡H

So that the plaintext is F and encipher to character T and by using ℰ -□-law sender is H ,so that I give more authentication by using ℰ -□-law,
Now to decipher, its means to repeats the plaintext is
□-□=max(min(26- ℰ -□,k),min(ℰ -□,26-k))
=max(min(26- 7,61),min(7,26-61))
=max(19,-35)
=19≡T
p=(□-□*k^{-1}) mod26
= (19*3) mod26
=5≡F
The □- variant Beaufort cipher steps for encipher and decipher (see Fiq(2))

4.12.Remarks:

1- In the situation if k<p the c-ciphertext , ℰ -□ and □-□ give the same value(characters) its mean the ℰ -□ and □-□ laws not work, now for example if we take p=7≡H ,k=3,k^{-1}=9 then

C=**21** , $\mathcal{E}$ -□=**21** , □-□=**21**,p=7≡H…….(see Fiq(4))
2- In the situation if k=p the ciphertext and □-□ give the different value(characters)and decipher not give the correct p-plaintext its mean the method not work ,now for example if we take p=21≡V, k=21,k^{-1}=5 then
p=21 ≡V . C=25 , $\mathcal{E}$ -□=5 , □-□=21 ,p=1≡B ≠

5. digital signature in public key cryptography by using $\mathcal{E}$ -□ and □-□ laws:

5.1. □ -Pohlig-Hellman cipher:

In the Pohlig-Hellman scheme, the modulus is chosen to be a large prime K, now by using $\mathcal{E}$ -□-law the enciphering functions are thus given by:

C=p^e mod k

$\mathcal{E}$ -□=max(min(26-c,k),min(c,26-k))

and by using □-□ law the deciphering functions are thus given by:

□-□=max(min(26- $\mathcal{E}$ -□,k),min($\mathcal{E}$ -□,26-k))

p= □-□ ^{d} mod k

and you can see the steps of encipher and decipher…….(see Fiq(4))

5.2.Example:

Let the plaintext (p=17≡R) , (k=29) secrete key So, to encipher
_ First we compute e-kept secret by
e=$d^{Ø(Ø(k))-1}$ mod Ø(k)
=$3^{Ø(28)-1}$ mod 28
=3^{11} mod 28
=19

Now encipher
C=p^e mod k
=17^{19} mod 29
=12≡M

$\mathcal{E}$ -□=max(min(26-c,k),min(c,26-k))
=max(min(26-12,29),min(12,26-29))
= max(14,-3)
=14

and by using □-□ law the deciphering functions are thus given by:

□-□=max(min(26- $\mathcal{E}$ -□,k),min($\mathcal{E}$ -□,26-k))
=max(min(26- 14,29),min(14,26-29))
=max(12,-3)
=12

p= □-□ ^{d} mod k
=12^3 mod 29
=17≡R

5.3. □ -Rivest-Shamir-Adleman(RSA) cipher:

In the RSA scheme,the modulus n is the product of two large primes r and q:
n=rq
thus
Ø(n)=(r-1)(q-1)
the enciphering functions are thus given by:
C=p^e mod n

$\mathcal{E}$ -□=max(min(26-c,n),min(c,26-n))

and deciphering functions are thus given by:

□-□=max(min(26- ℰ -□,n),min(ℰ -□,26-n))

p= □-□ ^{d} mod n

and you can see the steps of encipher and decipher…….(see Fiq(4))

5.4.Example:

Let the plaintext (p=8≡I) , (r=5,q=7,d=7) secrete key So ,n=r*q=5*7=35 to encipher

- First we compute e-kept secret by

$e=d^{Ø(Ø(n)-1}$ mod Ø(n)

$=7^{Ø(24)-1}$ mod 24

$=7^{Ø((2^{3})*3)-1}$ mod 24

$=7^{7}$ mod 24

=7

Now encipher

$C=p^{e}$ mod n

$=8^{7}$ mod 35

=22≡W

ℰ -□=max(min(26-c,n),min(c,26-n))

=max(min(26-22,35),min(22,26-35))

=max(4,-9)

=4

To decipher is

□-𝒜=max(min(26- ℰ -□,n),min(ℰ -□,26-n))

=max(min(26- 4,35),min(4,26-35))

=max(22,-9)

=22

p= □-□ ^{d} mod n

$=22^{7}$ mod 35

=8≡I

References:

[1]-Alfred J.Menezes,paul c.van Oorschot and scott A.vanstone, "Handbook of Applied cryptography",CRC press,1996.

[2]-Bruce,"application cryptography",second edition,published by john wiley and sons,inc,1996.

[3]-Dorothy E."cryptography and data security",by Addison Wesley publishing company,1982.

[4]-David M.B" Elementary number theory",second edition, wcb published 1989.

[5]-hans delfs and helmut knebl"introduction to cryptography",germany,2002.

[6]-J.Von zur Gathen"classical cryptography",bonn-Aachen international center technology,version:july 14,2008.

[7]-Jennifer S. and Josef p."cryptography: an introduction to computer security", by prentice hall of astralia pty,lid ,p.35-88,1982.

[8]- Jennifer S. and Josef p."cryptography: an introduction to computer security", by prentice hall of astralia pty,lid ,p.61-77,1989.

[9]-Kranak E."primality and cryptography",wiley-tentner series in computer science ,1989.

[10]-Rbit A. and Redfern E.J."introduction to number theory with computing", first published in great Britain,1989.

[11]-randy nichols"classical cryptography ",American,1995.

[12]-Shimada M.”Another practical public key, cryptosystem”, Electronics letters, vol. no.23,p. 2146-2147,1992.