Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 7, No. 3, October 2019, pp.1433-1438
Available online at: http://pen.ius.edu.ba

Soft public key Cipher

Ameer A. J. AL-Swidi[1], Enas Hamood Al-Saadi[2], Lamis Hamood Al-Saadi[3]
Department of Mathematical, College of Education for Pure Science, University of Babylon, Iraq.

Article Info

Received, 2019

Keyword:

Soft simple Knapsack,
Soft trapdoor Knapsack,
SNR,
PSNR.

ABSTRACT

Encryption in general is the process of keeping up the secrecy of data (both fixed and versatile) utilizing programs that can Convert and make an interpretation of that data into codes so that whenever got to by unapproved people doesn't They can comprehend anything since what appears to them is a blend of images, numbers and unlimited characters, the file is encrypted And decryption by password, which must be known to both parties (sender and receiver) This is called With symmetric encryption, Decryption means decryption. The quality and viability of encryption rely upon two key factors: the algorithm, and the key length evaluated by Bit, the higher the bit, the greater the security and difficulty of decrypting. The concept of soft set was studied and applied on the public key cryptography like simple Knapsack and Trapdoor Knapsack ciphers. Significant results were presented that was the measure of the evaluate encryption using the SNR and PSNR.

Corresponding Author:

Ameer A. J. AL-Swidi ,
Department of Mathematical,
College of Education for Pure Science,
University of Babylon, Iraq.
Email: ameer.alswidi@yahoo.com

1. Introduction

Moldtsov introduced in 1999 new mathematics to deal with the uncertainty concept of soft set Since this concept make the link between the set with the parameters of the set does not affect the current methods and be free of difficulties Since this theory has multiple applications has been previously proved by Moldtsov[1].Maji,p.k [2], from the theoretical side of soft sets, defined and studied many operations.Knapsack problem depending on the difficulty of solving that uses for either secrecy or authenticity, but not both the simple. Trapdoor Knapsack method depending on the Knapsack problem [3, 4]. The signal to noise ratio (SNR) is an appropriate yardstick that uses in the characterization of the physical layer performance. A high SNR at the receiver allows an accurate synchronization. Various modulation formats applies to exploit the high SNR available at receiver for decoding and This scale Peak signal-to-noise ratio (PSNR) is used which represents the light accuracy between the ratio of the maximum value of the signal potential forces with the power of noise sabotage [5-10].

2. Preliminaries

2.1 Definition
Let E be a set of parameters defined on the initial universal set I, called the pair (F, S) and defined on the set I by the soft set where F: S→P (I) is an mapping and P (I) represents the set of power for I as well S⊂E [1].
2.1.1 Example
Suppose the following:
I is a diplomatic men under consideration
E Represents a set of parameters and each parameter indicates either a word or a sentence

E={tall ,average length ,small ,black hair ,blonde hair ,fat man ,graceful man ,weak man ,black eyes ,blue eyes ,white skin ,black skin}

In order to define the soft set (F,S) in this case describes the attributes of the human, consider six men in the universe set I ,given by I={H_1,H_2,….,H_6} ,and let S={a_1,a_2,….,a_8}

such that a_1, a_2,….., a_7 and a_8 stand for the parameters: tall, small, black hair, blonde hair, black eyes , blue eyes, white skin and thin respectively.

Suppose that :F(a_1) ={H_3}, F(a_2) ={H_1,H_2}, F(a_3) ={H_4,H_5,H_6}, F(a_4) ={H_2,H_3}, F(a_5) ={H_2,H_6},F(a_6)={H_1,H_3,H_4},F(a_7)={H_1,H_3,H_4},F(a_8)={H_1,H_3,H_4}

{F(a_i),i=1,2,……8} subsets of the universe set I and a collection of approximate descriptions of an object that dealt with table.

Table1: tabular representation of a soft set

E U	Tall	small	Black hair	blonde hair	black eyes	blue eyes	white skin	thin
H_1	0	1	0	0	0	1	1	1
H_2	0	1	0	1	1	0	0	0
H_3	1	0	0	1	0	1	1	1
H_4	0	0	1	0	0	1	1	1
H_5	0	0	1	0	0	0	0	0
H_6	0	0	1	0	1	0	0	0

2.2 Knapsack cipher

Based on NP-complete Knapsack cipher, the declared key encryption can be described in three methods, for the first and second method Use them not for authentication but for secrecy, whereas third method was used for authentication but not for secrecy, Shamir [3] studied the feasibility of construction, Merkle and Hellman (1978) propose a public-key system using Knapsack problem [4] by given A={a1,a2,….,an} positive integer and find the positive integer C (cipher text) by C=A.M or C=$\sum_{i=1}^{n} a_i m_i$,M={m1,m2,….mn} is represent the plaintext (Message)

for example if

A={10,8,17,20,15,9,6} and M={1,0,1,1,0,0,0}

then C=10+17+20=47

The knapsack algorithm is one of the best algorithms to solve arbitrary instances of size n require O($2^{n/2}$) time, in a simple Knapsack (super increasing) it solved in linear time algorithm snap (C,A):

("simple Knapsack algorithm")

for i:= n down to 1 do

begin

if C≥ ai then mi=1 else mi=0

C:=C-ai*mi

end;

if C=0 then snap:=M else " no solution exists "

2.2.1 Example

given A=(1,3,5,10,22) and M=(1,1,0,1,0)

then

to encipher is :

C=A*M=(1+3+10)=14

to decipher is :

C= 14<22 then m5=0

=14-22*0=14

C=14>10 then m4=1

=14-10*1=4

C=4<5 then m3=0

=4-5*0=4

C=4>3 then m2=1
=4-3*1=1
C=1≥1 then m1=1
∴ M=(m1,m2,m3,m4,m5)=(1,1,0,1,0)

2.3 Trapdoor Knapsack

Merkle and Hellman convert it to a Trapdoor Knapsack [4], which hard to solve
-choose A=(a_1,a_2,….a_n) , $a_i > \sum_{j=1}^{i-1} a_j$
-choose $U > 2a_n > \sum_{i=1}^{n} a_i$
-choose W so that gcd(U,W)=1
-compute $W^{-1} = W^{\varphi(u)-1}$ mod U
-compute E_A=W*A mod U
Where E_A is public-key,A and W^{-1} are secrete
to encipher is :
C=E_A*M
To decipher :
C'=w^{-1}*C mod U
you have A and C' solve linearly form
C'=A*M

2.3.1 Example:

if A=(1,3,5,10)
- U=20
- W=7 , gcd(7,20)=1
- then $W^{-1}=W^{\varphi(U)-1}$ mod U
=$7^{\varphi(7)-1}$ mod 7
=7^{6-1} mod 7
=3
- E_A=(7,1,15,10)≡ (7*1 mod 20 , 7*3 mod 20 ,7*5 mod 20 ,7*10 mod 20)

let the plaintext (M=13) then M=(1,1,0,1)
to encipher is:
C=E_A*M=(7+1+10)=18
to decipher is:
C'=C*W^{-1} mod U =3*18 mod 20 =14
C'=A*M=14=(1,3,5,10).M
by snap(14,A*M) ,we get
M=(1,1,0,1)

2.4 Soft simple Knapsack

In this method, deal with the some attributes in human as h_1,h_2,….,h_6 and applied the cipher in simple Knapsack algorithm as example:
let A=(1,3,5,10,20,80,160) and H_1=(01000111)
to encipher is:
, then C=1*0+3*1+5*0+10*0+20*0+40*1+80*1+160*1=283 $C=\sum_{i=1}^{n} a_i h_i$
to decipher is:
C=283>160 then h_8=1
=283-160*1=123
C=123>80 then h_7=1
=123-80*1=43
C=43>40 then h_6=1
=43-40*1=3
C=3<20 then h_5=0
=3-20*0=3
C=3<10 then h_4=0
=3-10*0=3
C=3<5 then h_3=0

=3-5*0=3
C=3≥3 then h_2=1
=3-3*1=0
C=0<1 then h_1=0
=0-1*0=0
∴ H_1=(01000111)
In similar way to compute $H_2,H_3,\ldots,H_6$

Table2:tabular representation of a Soft simple knapsack

U	$(F(e_1),F(e_2),\ldots F(e_8))\equiv(h_1,h_2,\ldots,h_8)$	$C_1,C_2,\ldots C_6$
H_1	(01000111)	283
H_2	(01011000)	33
H_3	(10010111)	291
H_4	(00100111)	285
H_5	(00100000)	5
H_6	(00101000)	25

2.5 Soft Trapdoor Knapsack

In the same manner of soft simple Knapsack . as example
if
- A=(1,3,5,10,20,80,160)
- U=320
- W=7 ,gcd(7,320)=1
- compute $W^{-1}=7^{\varphi(320)-1}$mod320
  $=7^{63}$mod320=183
- E_A=W*A mod U
  =(1*7 mod 320,7*7 mod 320,5*7 mod320,10*7mod320,20*7 mod320,40*7mod320,80*7mod320,160*7 mod320)
  =(7,21,35,70,140,280,240,160)

let H_1=(01000111) then
to encipher is:
C=E_A*H=701
to decipher is:
C'=C*W^{-1} mod U
=701*183 mod 320=283
C'=A*H_5=5=(1,3,5,10,20,40,80,160)H_1
by snap(5,A.H_5) ,we get
H_1=(00100000)
in similar way to compute $H_2,H_3,\ldots,H_6$

Table3:tabular representation of a Soft Trapdoor Knapsack

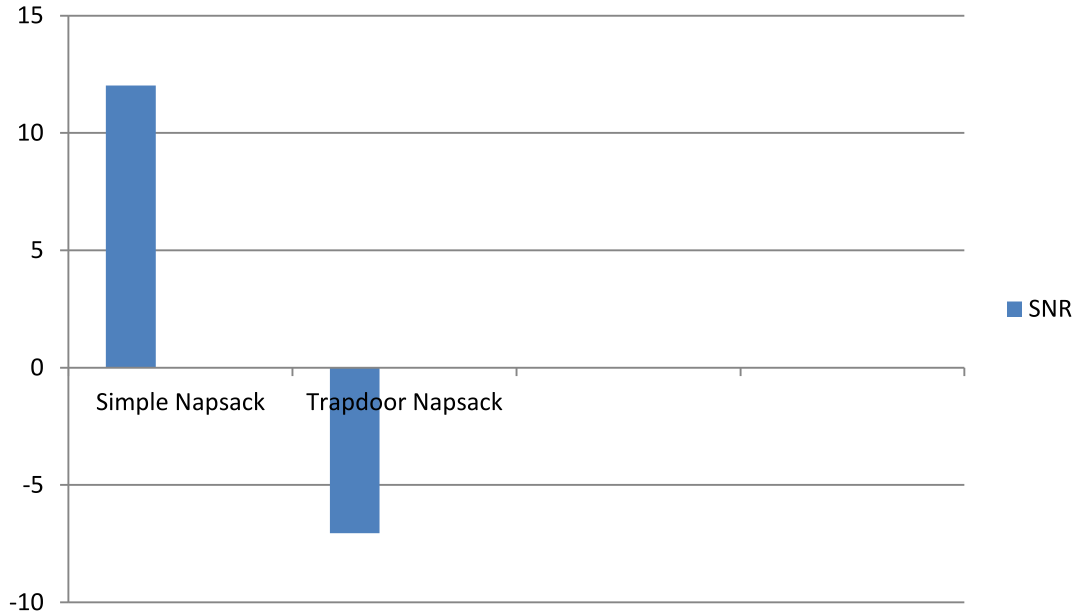
U	$(F(e_1),F(e_2),\ldots F(e_8))\equiv(h_1,h_2,\ldots,h_8)$	$C_1,C_2,\ldots C_6$
H_1	(01000111)	701
H_2	(01011000)	231
H_3	(10010111)	757
H_4	(00100111)	715
H_5	(00100000)	35
H_6	(00101000)	175

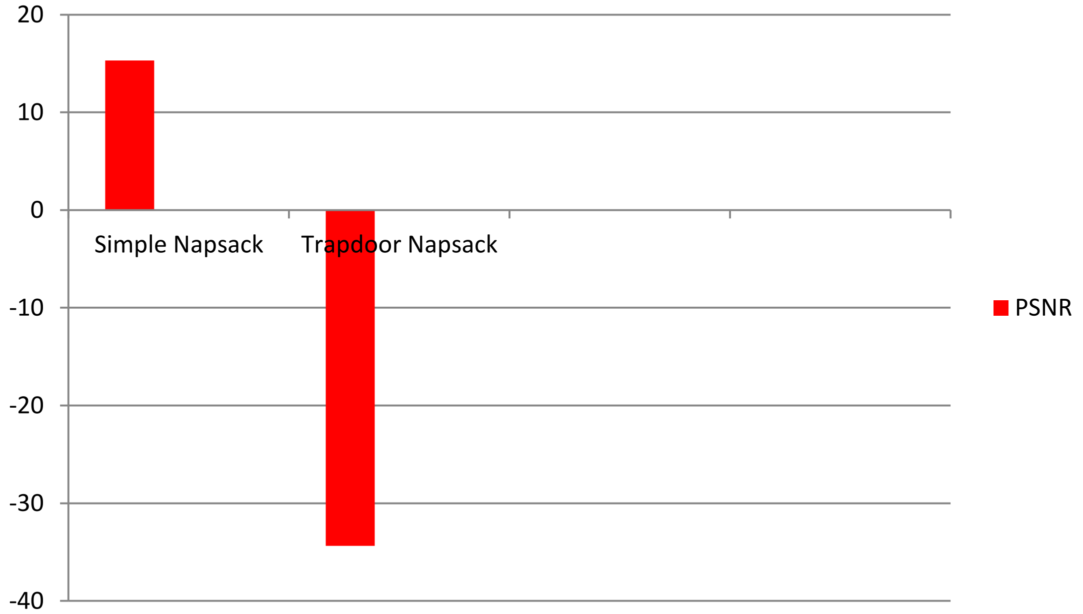
3. Measurement (SNR and PSNR)

In this section we will explain the measurement of SNR and PSNR shown in the following table:

Table4: tabular representation of measure SNR and PSNR

measure / Knapsack types	SNR	PSNR
Soft simple Knapsack	12.0261	15.29
Soft trapdoor Knapsack	-7.0559	-34.37





4. Conclusions

We calculated during the calculation of the SNR and in contrast to his PSNR that the ratios of the difference between the two methods are different where in the simple Knapsack cipher that the difference was more than 3 which is a reasonable rate and is a method is noticeable compared with the soft Trapdoor Knapsack which gave very good ratios more than 27 and therefore more reliable in Encryption method which gives more security and all this can be seen in the previous table .

References:

[1] P. Sundarayya and G. Vara Prasad, “A public key cryptosystem using Affine Hill Cipher under modulation of prime number,” Journal of Information and Optimization Sciences, vol. 40, no. 4, pp. 919–930, May 2019.

[2] S. Sadeghi and N. Bagheri, “Security analysis of SIMECK block cipher against related-key impossible differential,” Information Processing Letters, vol. 147, pp. 14–21, Jul. 2019.

[3] I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, “Modified RSA-based algorithm: A double secure approach,” Telkomnika (Telecommunication Comput. Electron. Control., vol. 17, no. 6, pp. 2818–2825, 2019.

[4] M. A. Maricar and N. P. Sastra, “Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi,” Majalah Ilmiah Teknologi Elektro, vol. 17, no. 1, p. 59, Mar. 2018.

[5] S. B. Thigale, R. K. Pandey, P. R. Gadekar, and V. A. Dhotre, “Lightweight novel trust based framework for IoT enabled wireless network communications,” Period. Eng. Nat. Sci., vol. 7, no. 3, pp. 1126–1137, 2019.

[6] Y. Wei, P. Xu, and Y. Rong, “Related-key impossible differential cryptanalysis on lightweight cipher TWINE,” Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 2, pp. 509–517, Jan. 2018.

[7] R. M. Marzan, “Randomness Analysis on Enhanced Key Security of Playfair Cipher Algorithm,” International Journal of Advanced Trends in Computer Science and Engineering, pp. 1248–1253, Aug. 2019.

[8] L. Kraleva, V. Rijmen, and N. L. Manev, “Correlation Distribution Analysis of a Two-Round Key-Alternating Block Cipher,” Tatra Mountains Mathematical Publications, vol. 73, no. 1, pp. 109–130, Aug. 2019.

[9] H. Jiao, T. Pu, L. Shi, Y. Chen, and L. Yu, “A novel realization of quantum stream cipher with key-modulated local light,” Optical Fiber Technology, vol. 53, p. 102007, Dec. 2019.

[10] S. Park, J. Kim, K. Cho, and D. H. Yum, “Finding the key length of a Vigenère cipher: How to improve the twist algorithm,” Cryptologia, pp. 1–8, Oct. 2019.