RESEARCH ARTICLE OPEN ACCESS

A Survey on Diverse Techniques of Encryption in Practice

Ashish Pareek, Prof. John Singh
School of Information Technology & Engineering, VIT University, Vellore, Tamil Nadu, India
School of Information Technology & Engineering, VIT University, Vellore, Tamil Nadu, India

ABSTRACT
This converse will attend a perception on the contemporary state of play in the fallow of encryption algorithms in meticulous way (on private key block ciphers) what're comprehensively used for majority of data and link encryption. Primarily, survey of the more prevalent and thought-provoking algorithms at present in use was carried out. This endeavor stress essentially on a number of encryption techniques that are manageable & comparative study of all techniques unruffled as a literature survey. Aim a wide-ranging experimental study of operations of various available encryption techniques. Also emphases on image encryption techniques, data encryption techniques. This study encompasses the routine constraints used in encryption processes and scrutinizing on their safety issues.
Keywords: Encryption, Integrity, Security

I. INTRODUCTION

The h igh grow th in the netw orking technology leads a common cult ure for interchanging of the da ta very drastic ally. Hence it is m ore vulnerable of dupl icating of da ta a nd re -distributed by hac kers. Therefore the inform ation has to be protected while transmitting it, Sensitive infor mation like credi t car ds, banking transa ctions an d social security numbers need to be protected. For this many encryption techniques are existi ng which are use d to avoid the infor mation theft . In rece nt days of wireless communication, the encryption of data plays a major role in s ecuring the d ata in online transmission focuses mainly on its security across the wireless. Different encryption techniq ues are use d to protect the confid ential data from unautho rized use. Encryption is a very c ommon techniq ue for promoting the infor mation security. The evolution of encryption is movin g towa rds a f uture of endless possibilities. Everyday new met hods of encry ption techniques are disco vered. This paper ho lds some of those recent existing encryption techn iques and th eir security is sues. The perform ance of all t hose encryption tech niques are stu died and discus sed including UMA RAM and U R5 in la ter cha pters of the paper.

A. Basic Terms Used in Cryptography Plain Text

The original message that the pers on wishes to comm unicate with t he ot her is d efined as Pla in Text. In Cryptography the a ctual mes sage that has to be sen d to the ot her end is g iven a sp ecial name as Plain Text. For example, Alice is a p erson wishes to send "Hel lo Fri end ho w are you " mess age to the person B ob. Here "H ello Fri end how a re y ou" is a plain text message.

Cipher Text

The mess age that cannot be unde rstood by anyone or meanin gless mes sage is w hat we cal l as Cipher Text. In Cryptography the ori ginal message is transformed in to n on read able me ssage before the transmission of actual mes sage. For exa mple, "Ajd672#@91ukl8*^5%" is a Ciph er Te xt produced for "Hello Friend how are you".

Encryption

A proc ess of conv erting Plain Te xt into Cipher Te xt is c alled as Encryp tion. Cryptography uses the encryptio n techn ique to send confidential messages thro ugh an ins ecure channe l. The proce ss of encr yption re quires two thing s- an encrypt ion algorithm and a key . An encryption algorithm me ans the tec hnique th at has b een us ed in encry ption. Encryption takes place at the sender side.

Decryption

A rev erse proc ess of encryptio n is camlled as De cryption. It is a proc ess of c onverting Cip her Text into Pla in Text . Cryptography uses the decryption technique at the receiver side to obtain the original message from non read able message (Cipher Text). The process of decryption requires two things- a Dec ryption algorit hm and a key . A Decr yption algorithm mea ns the techique th at has be en use d in Decryption. Generally the encrypt ion and decrypt ion algorithm are same.

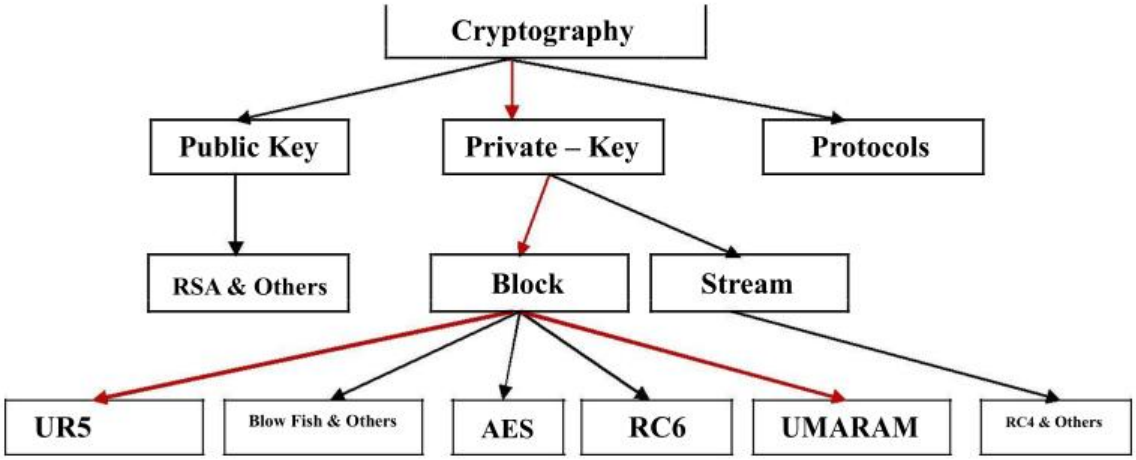

Fig.1.1 Overview of Most Common encryption algorithm

KEY

A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes pla ce on the Ci pher T ext. The se lection of key in Crypto graphy is ver y important since the secu rity of encryp tion algo rithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the P lain Text "Pres ident" then Cipher Text produced will be "Suhvlghqw".

B. Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

Confidentiality

Information in comput er is tra nsmitted and has to be acc essed on ly by the a uthorized pa rty and not by anyone else.

Authentication

The information received by any system has to che ck the id entity of the sende r that whet her the information is arri ving fro m a authori zed person or a false identity.

Integrity

Only the authori zed party is allow ed to modify the trans mitted informa tion. No on e in between the sen der and recei ver are allo wed to alter the given message.

Non Repudiation

Ensures that ne ither the sen der, nor the receiver of messa ge shoul d be ab le to de ny the transmission.

Access Control

Only the auth orized part ies a re a ble to access the given information.

C. Classification of Cryptography

Encryption algorithms can be classified into two broad categories- Symmetric and Asymmetric key encryption.

Symmetric Encryption

In symmetric Cryptography the key used for encryption is sim ilar to the key us ed in decryp tion. Thus, the key distribution has to be made prior to the transmission of information. The key play s a ve ry important role in sym metric crypto graphy since their security directly depends on the na ture of key i.e. the key len gth etc . There are va rious sym metric key algorithms su ch as D ES, TRIPLE D ES, AES, RC4, RC6, and BLOWFISH [2].

II. PREVIOUS RELATED WORKS

This subsecti on descri bes and exami nes previous w ork on mo st comm on algo rithm implementation for both softw are and hard ware approaches. The metrics ta ken into conside ration are processing sp eed, throughput, power consump tion, packet size and data types.

Evaluating the Effe cts of Crypto graphy Algorithms on pow er con sumption for wirel ess devices has d one by D . S. Abdul. Elminaam et .al. (2009) presents a per formance evaluat ion of selec ted symmetric encryption algorithms.

Comparison Of Data Encryption Algorithms has done by Simar Preet Singh , and Ra man Maini -

The sim ulation re sults showe d that Blow fish has better performan ce than ot her commo nly used encryption alg orithms. AES showed poor performance res ults compared to other algorith ms, since it requires more proce ssing power. The first set of expeiments were conducted using ECB Mode. The resmults sho w the super iority of Blow fish algor thm over othe r algorithms in term s of pro cessing time . It shows also that AES co nsumes more reso urces when data block size is relatively big. Another point can be noticed he re tha t 3DES req uires al ways m ore tim e than DES becau se o f it s tr iple pha se enc ryption characteristic. Blowfish, which has a lo ng key (448 bit), outperformed other encryp tion alg orithms. DES and 3DES are kn own to hav e wor m hole s i n their security mechan ism, Blowfish and AES d o not have any so far [6].

As expected, CBC requires more proce ssing time than ECB beca use of its ke y-chaining na ture. The results indicates also that the ex tra time added is not sign ificant for m any appli cations, knowing that CBC is much better than ECB in terms of protection.

Evaluation Of Performance Chara cteristics Of Crypto system Using Text Files designed by challa Narasimham and Jayaram Pradhan (2008) - They perf ormed the perfor mance comp arison for variable si zed text file s as inp ut. An analysis on computational running time s re sults i n significant difference among the me thods. He believe in that the performance of DES , especially in dec ryption method is very hi gh than the alterna tives. Despite the key distr ibution, DES is mor e suit able to the application, which h as the decryption as the high est priority.He has propos ed and perfo rmed t he test cases on the two PKCS methods i .e., RSA and NTRU Thou gh the encrypt ion, decryption and complexity are hig h in NTRU , the RSA provides the highest sec urity to the bu siness applicati on. He presented all these param eters with computa tional running time s for all the meth ods, so as to select the appropriate method [7].

Abdel-Karim and his colleague Al Tamimi presented simula tion res ults showed that Blow fish has a bet ter perfo rmance than other co mmon encryption algorith ms used . Since Blowf ish has n ot any kn own sec urity weak poin ts so far , whichh makes it an excel lent can didate to be considered as a standard encryp tion alg orithm. AES sho wed po or performance res ults com pared to oth er algorithms since it require s more process ing power . Using CBC mode has added extra pro cessing time , but over all it was relat ively negligible especi ally for cert ain application that requ ires more secure encryption to a relatively large data blocks.

The results showed that Blowfish has a ve ry good perf ormance comp ared to other algor ithms. Also it show ed tha t AES has a b etter perfo rmance than 3DES and DES . Amazingly it sh ows also th at 3DES has al most 1/3 throughput of DES , or in oth er word it ne eds 3 times t an DES to proces sthe sam e amount of data [8].

P. Prasithsangaree and his collegeue P. Krishnamurthy have anal yzed the Energ y Consumption of RC 4 and AES Algorit hms in Wireless LANs in the ye ar 2003.They have evaluated the perfor mance of RC 4 and AES encrypt ion algorithms. The perfor mance metrics w ere encryption thro ughput, CPU work load, energy cos t and key size va riation. Experiments sho w that th e RC4 is fa st and energy efficient for en crypting large packets. However, AES was more effici ent than RC4 for a smaller pack et size. From the results, it appears that we can save ener gy by using a combination of RC4 and AES to provide enc ryption f or a ny packet size. The tradeoffs with security are n ot complet ely clear[9].

Comparative Anal ysis of A ES and RC 4 Algorithms for Be tter Utili zation has desig ned by Nidhi Singhal , J.P.S.Raina in th e ye ar (2011).The performance me trics were throug hput, CPU pr ocess time, memory utiliz ation, encryption and decr yption time a nd key size vari ation. Experiments show that the RC4 is fast and e nergy efficmient for encr yption and decryption. Based on the analysis mdone as p art of the research, RC4 is be tter than AES .we compare the encryption time of AES a nd RC4 algorithm over different pac ket size. RC4 takes less ti me to encry pt files w.r.t. AES. In AES, CFB and CBC takes nearly similar ti me but E CB tak es les s ti me then both of these [10].

The result sho ws the superi ority of RC 4 over AES. With different key sizes RC4 gives almost the s ame result . But for diff erent modes of AE S, throughput de creases as ke y size incre ases because of m ore usage of comp utational po wer and encryption characte ristics. Thus RC 4 in nature consume le ss po wer w .r.t its count rparts. Better results were obtaining in decryption w.r.t. encryption

Efficiency and Sec urity of S ome Im age Encryption Algo rithms Marwa Abd El -Wahed et .al (2008) – worked in this paper, four image encryption algorithms have been studied by means of meas uring the encryption quality, the memory requirement, and the execution time of the encryption. In addition, the security an alysis of these sche mes is investig ated from cryptog raphic vie wpoint; statistical and differential attacks . The res ults are comp ared, focusing on t hose porti ons where ea ch sch eme is performed differently. Based on the experim ental results, it can be concluded that:

1) Permutation te chniques ac hieve eff icient schemes (minimum encrypti on time and memory require ment) compared wit h substitution techniques.

2) Techniques that b ased on SCAN methodo logy achieve the highest security.
3) The cha os-based encry ption scheme s till need further stu dy to achiev e a reas onable de gree of security and acceptable efficiency.
4) A secu rity defect exists in the sche mes t hat generated k eys on ran dom number seq uence compared with the techniques that based on scan methodology.
5) When permu tation techn ique comb ined with substitution technique in intertwined manner and iteratively, it leads to design complex, but secure and effic ient techn iques w hen variable key size and key num ber is use d (according to plain - image size).
6) The schemes implem entation usi ng the computational appro ach for selectin g andom permutations performs slower time.
7) If the key used to encr ypt plaint -image is random and the len gth of the ke y exce eds the amount of pl aint image to be encryp ted, then the cipher-image is unbreakable.

From t hese resu lts it appea rs th at there are three m ain crit eria should be conside red at the same level of imp ortance to ev aluate ne w cryptosy stems: how much it eases impleme ntation, level of secu rity, and efficie ncy. To identify an opti mal sec urity le vel, it is neces sary t o comp are caref ully the co st of the multimedia inf ormation to be protecte d and the cos t of the protection itself [11].

A Comparative Stu dy o f T wo Sym metric Encryption Algo rithms Acros s Dif ferent Platfor ms designed by S .A.M Rizvi 1 et.al. All algorith ms r un faster on Wind ows XP. The CAST ru ns slo wer t han AES for text . Blowfish encr ypts imag es most efficiently on all 3 platforms, even CAST run s fas ter on Wi ndows XP for ima ge d ata. But on Wind ows Vista and 7, AES and CAS T perf orm at the s imilar speed .CAST per forms bett er t han BLOW FISH a nd AES on Wind ows XP for encry pting au dio files at Windows Vista, and significant difference on Windows 7 in perfor mance of CA ST and AES , however BLOW FISH as encryption of audio files at less speed happens [12]. Performance Evaluati on of Three Encr yption/Decryption Algorithm s on the SunOS and Lin ux Operating Sys tems Turki Al - Somani et .al. They pres ented an im plementation of three sym metric block encryptio n algorit hms u sing Java and JC A. The ma in obje ctive was to evaluate the performance of these algo rithms in ter ms of CPU execution time . The measure ments were perfor med on t wo platforms ; SunOS and Linux . The analy zed time wa s the CPU executio n time for gene rating the secret key , encryption and decr yption on a 10MB file. The results sho wed that the Blow fish algo rithm was the fast est algorith m followed by the DES algorithm the n the Tr iple-DES algor ithm. The Triple-DES algorith m was slow in its perfor mance due to the add ed comple xity and securit y it has over the DES algorithm.

ThroughPut Analysis of Vario us Encryption Algorithms present ed by Gurjeevan Si ngh et al ., (2011)- For expe riment a Lapt op with 2.20 GHz C.P.U., 4GB RAM Core-2-Dou Processor and Windows 7 Home Premi um (32-Bit) is us ed in whichh the perform ance data are col lected. In this experiment soft ware encr ypts the t ext file si ze that ranges fr om 20 Kb to 99000 Kb. Their implementation is thoroughly teste d and is optimized to give the maxim um perfor mance for the algorithm.The performance ma trices are throug hput. The through put of encrypt ion as we ll as decrypt ion schemes is calcu lated but one by o ne. In the ca se of Encryption sc heme through put is calculated as the average of total plain text in k byt es divi ded by the average Encr yption time and in the ca se of Decryption sc heme throughp ut is calcu lated as the average of t otal cip her text is divide d by the av erage Decryption time. This work presents the performance evaluation of se lected sy mmetric algo rithms. The selected alg orithms are AES , 3DES, Blowfish and DES. The pr esented simul ation result s sh ow the numerous poi nts. Firstly, it w as conc luded that Blowfish has bett er perform ance than o ther algorithms fo llowed by AES in terms of throughput . Secondly 3DES has least efficient of all the studied algorithms [15].

R. Chandramouli et .al. investigated batt ery power-aware Encry ption alg orithms. The ma in conclusmions they rea ched wa s that the po wer consumption cha nges linea rly with the nu mber of rounds of seve ral po pular crypto graphic algorithms . Their experimental test bed had a laptop connected to a power supply . The po wer supply was connected to a computer running the Lab VIEW soft ware to gr aph changes in voltage and curr ent from the power supply. These change s were grap hed during the li fe of the encryption algorithms [16].

Shashi Mehrotra Seth and her collegue Rajan Mishra (2011) jointly has done a Compa rative Analysis Of Enc ryption Algo rithms For Data Communication.The auth ors analyse the performance of encr yption algor ithm is evaluat ed considering the follo wing paramemters like Computation Time , Memory usa ge and Output Bytes. The experime ntal res ults shows the comparison of three algorit hm AES , DES and RSA using s ame text fi le for five experi ment, output b yte for AES a nd DES is sam e for diffe rent sizes of files . The authors noticed the RSA has very sm aller output byte compar e to AES and DES algo rithm. Time taken by RSA algori thm is m uch higher compare to the tim e taken by AES and DES algo rithm. Finally the aut hors con cludes, Based on the t ext fil es used

and the exp erimental re sult it was conc luded that DES algor ithm consu mes least encr yption time and AES algori thm has least mem ory u sage while encryption time differen ce is very mi nor in case of AES algo rithm and DES algor ithm. RSA cons ume longest encr yption ti me and m emory us age is also very hig h but outp ut b yte is l east in ca se of RSA algorithm [17].

Diaa Salama Abd Elminaam etal. (2010) [18] eavaluate the Performan ce of Symme tric Encryption Al gorithms like AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. A compar ison has been cond ucted for those encry ption algori thms at different settings for each algorith m such as differe nt sizes of data blo cks, diferent dat a typ es, battery power consum ption, different key size and finally encryption/decryption speed. For the experi ment, the authors use a lapt op IV 2.4 GHz CPU , in whi ch performance data is collected. In the experiments, the laptop encrypts a differe nt file size ra nges from 321 K byte to 7.139Mega Byte 139MegaBytes for text data, from 33 Kbytes to 8262 Kbytes for audio data, and from 4006 Kbytes to 5073 Kbytes for video files. By the authors, several points can be concluded from the Experimental results. The RC6 requires less time than all algorithms except Blowfish. The AES has an advantage over other 3DES, DES and RC 2 in terms of time consumption and throug hput. 3DES has lo w performance in ter ms of pow er c onsumption and throughput when co mpared with DES . It alwa ys requires m ore t ime than DES becmause of its tr iple phase encryption c haracteristics. Fnally, it is fou nd that RC 2 has lo w perf ormance and low th roughput when compared with other fiv e algorithms in spite of the small key size used.

Diaa Salama et .al joi ntly d one a re search work in the title “Wireless Network Security Still has no Clothes” [19]. The above researc h wor k ev aluate the performanace of most com mon symmetr ical encryption algor ithms like AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC 6. The author’s illustrates the key conc epts of secur ity, wireless networks, and securit y over wir eless netwo rks. Wireless se curity is dem onstrated by appl ying the common sec urity standard s like (802.11 WEP and 802.11i WPA, WPA2) and provides evaluation of six of the most common encryption algorithms on po wer consumption for Wirel ess device s na mely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6.

A com parison is condu cted betw een the results of selec ted diff erent encryption algorith ms using different setti ng such as diff erent and d ata types, different pack et siz e, different ke y siz e. In case of ch anging pa cket size, (throughput, power consumption in µJoule/Byte and p ower cons umption by c alculating diffe rence in bat tery perce ntage w re calculated) in case of en cryption pro cesses to calculate the performmance of each encrypti on algorithms. In case of chang ing data type s such as audio, throughput ,power consu mption in µJoule/Byte and power con sumption by calcu lating difference in batt ery perce ntage were calcul ated)in case of encry ption pro cesses to calcul ate the performance of each encryption algorithms.

Ruangchaijatupon.P and his col logue Krishnamurthy.P (2001) [20] has do ne a resear ch work on "Encryption and Po wer Consu mption in Wireless LANs” . This re search was sh own in that energy cons umption of dif ferent com mon symme tric key encryptions on ha ndheld devices. It is fou nd that after on ly 600 encryptions of a 5 MB fil e using Triple-DES the rema ining battery power is 45% and subsequent encry ptions are not p ossible as the battery dies rapidly . It was concluded in that AES is faster and more efficie nt than other encr yption algorithms. When the trans mission of data is considered there is insig nificant differ ence in performance of dif ferent symmetric key schem es. Increasing the key s ize by 64 bits of AES leads to increase in ene rgy consu mption about 8% without any data transfer. The difference is not noticeable.

Prasithsangaree.P and Krishnamurthy.P (2003), “[21] has done the anal ysis of Ene rgy Consumption of RC 4 and AES Algo rithms in Wireless LANs. A stu dy is con ducted f or diff erent secret key algo rithms such as DES , 3DES, AES, and Blowfish. They were impleme nted, and th eir performance was comp ared by encr ypting in put file s of varyi ng cont ents and s izes. The algor ithms we re tested on two dif ferent hardwa re pla tforms, to compare their pe rformance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The re sults sh owed that Blow fish had a ve y good perfo rmance c ompared to oth er algor ithms. Also it showed that AES had a bett er performa nce than 3DES and DES . It also shows that 3DES has almost 1/3 throughput of DES , or in other wor ds it needs 3 times than DES to p rocess the s ame amount of data.

Idrus.S.Z, Aljunid.S.A, Asi.S.M(2008), done the rese arch [22]work in the dif ferent bro wsers for evaluate the Perform ance Analy sis of Encryp tion Algorithms Te xt Leng th Size . The au thors study of security mea sure lev el has been prop osed for a web programming lang uage to analyze four W eb browsers. This study consider of measur ng the performances of encryp tion pr ocess at the programming lan guage’s scr ipt with the We b browsers. Gast.M.S (2002),"802.11 Wireless Network: The Definit ive Guide ,[23]" A study is conducted for different popular secret key algorith ms such as RC 4, AES, and XOR . They were implemented, and their perform ance was com pared by encryptin g for re al ti me vide o stre aming of

varying con tents. The res ults sho wed; encryption delay ove rhead using AES is less tha n the overh ead using RC4 and XOR algorit hm. Therefore, AES is a feasible soluti on to secu re real time video transmissions.

Monika Agr awal et al . 2012 gives a detmailed stu dy[24] of the popu lar symm etric k ey encryption algo rithms suc h as DES, TRIPLE DES , AES, and mBlowfish. Symmetric Key algorithms run faster than Asymmetric Key algori thms such as RSA etc and t he mem ory requirement of Sym metric algorithms is lesser th an Asymm etric encr yption algorithms. Further, the security aspect of Sym metric key encr yption is super ior than Asy mmetric key encryption.

Ezedin Barka and his collegue Moha mmed Boulmalf con ducting two expe riments[25] scenarios that were conduc ted for the purpose of establishing a baseline and for unde rstanding the im pact of adding encryptions, with diffe rent key siz es, used by WEP and WPA se curity protoc ols on UDP a nd TCP WLAN traf fic. While the first experi ment was for measuring the th roughput under normal conditio ns (No encryption appl ied), the second experim ent w as to analyze the variation of traffic throughputs over an Infrastructure networ k whe n encry ption is appli ed. the ge neral observa tions taken from these experiments are: Throughput decr eases when security, WEP and WPA are enab led. This is due to the fact that encry ption operati ons perfo rmed by these pro tocols incr ease the amount of data transmitted and slow do wn the rate of data being sent or received.

For WEP , when the ke y size in creases the throughput sligh tly decreas es, which is due to the fact that WEP ad ds the Init ial Value of its symm etric encryption key to the data sent and it use s the rest of the key bits to init iate a key sched uling al gorithm that gen erates a stre am key for the strea med data to be XORed with . This nor mal process of the RC 4 encryption algorithm can imp ose so me d elay to the data to be se nt a fter encry ption then recei ved and decrypted.

In the wirel ess to w ireless environment, the throughput suffered more degradation than that in the wireless to wired environment. This is due to the fact that in the wire less to wireless environment, there are double encryptions w hich res ult fro m havi ng two air interfaces with one acces s point. In th e ad hoc communication, the throughput is already low d ue to the fact that, in addition to the degradation caused by the encryption, there are no acce ss points involved in the commun ication process . Finally, general observation from all exper iments condu cted here indicate that there is s ome degradati on in thro ughput resulted from app lying encryption , however, this degradation is moderate, in comparis on to the benefits provid ed by a pplying encry ption, thus, we recommend that WEP or WPA encry ptions be enabled in WLANs comm unications[26].

D. S. Abdul. Elminaam etal., (2009) analysed the Perform ance Eval uation of Symm etric Encryption Algorith ms. The auth ors use a laptop IV 2.4 GHz CPU , in wh ich perfor mance data is collected. In the expe riments, the laptop enc rypts a different file siz e range s from 321 K byte to 7.139Mega Byte . Several per formance met rics are collected: encryption time , CPU p rocess t ime, and CPU clock cycles and battery power.

The following tasks that will be performed are shown as follows:

- A compar ison is con ducted between the res ults of the selected differe nt encry ption and decryption sche mes in terms of the en cryption time at two diffe rent e ncoding bas es nam ely; hexadecimal base encod ing and in base 64 encoding.
- A stu dy is perf ormed on the effect of ch anging packet size at p ower consu mption during throughput for e ach sele cted cryptography algorithm.
- A study is perfor med on th e effect of chang ng data type s - such as text or document and images- for each cryptography sel ected algorithm on power consumption.
- A study is performed on the effect of changing key size for cryptography selected algorithm on power consumption.

The selec ted algor ithms are AES , DES, 3DES, RC6, Blowfish a nd RC 2. Several poin ts ca n be concluded fro m the simulation results . First; there is no signi ficant differ ence when the re sults are displayed either in hexade cimal base enco ding or in base 64 encoding.

G. Ramesh et.al designed al algorithm in the year 2010 named as UMAR AM[27]. The UMA AM is a Sym metrical encrypt ion alg orithm. The k ey generation g enerates 16-keys dur ing 16-rounds.One key of them is used in one ro und of the encryption or decryption pr ocess. The n ew algo rithm uses a key size of 512-bits to enc rypt a plai ntext of 512-bits during the 16-rounds. In this Algori thm, a seri es of transformations h ave been used depending on S - BOX, different sh ift proce sses, XOR-Gate, and AND-Gate. The S-Box is used to map the inp ut code to an other c ode at the ou tput. It is a mat rix of 16×16×16 .The S-Box consists of 16-slides, and each slide havin g 2-D of16×16 . The numbers fro m 0 to 255 are arran ged in rand om po sitions in each sli de. G. Ramesh et .al designed al algorit hm in the year 2010 named as UR 5[28]: A block encr yption algorithm is propo sed in this appr oach. In thi s Algorithm, a series of transf ormations ha ve bee n used depe nding on S -BOX, XOR Gate , and AND

Gate. The proposed algorithm encrypts a pl aintext of size 64-bits by a key size of 64-bits. It uses eig ht rounds for en cryption or decryp tion process . It overcomes some drawbacks of the other algorithms.

III. CONCLUSION

In this er a, the securi ty for the d ata has become hig hly impor tant since the commu nication by transm itting of dig ital pr oducts over the open nemtwork occur very frequently. In this paper, it has been sur veyed th at the ex isting works on the encryption techniques. Those enc ryption tec hniques are stu died and analyzed well to pr omote the perfrmance of th e encryption met hods also to en sure the sec urity proceedings . To su m u p, all th e techniques are us eful for re al-time encrypt ion. Each technique is uniq ue in its o wn way, which might b e suitable for diffe ent appli cations. Everyday new encryption techni que is evolving he nce fast and secure con ventional encry ption techniq ues will always workout with high rate of security.

REFERENCES

[1] William Stallings "Netw ork Secu rity Essentials (Applications and Stan dards)", Pearson Education, 2004.

[2] National Bureau of Standards , "Data Encryption Standard," FIPS Publication 46, 1977.

[3] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[4] Ramesh G , Umarani. R" Dat a Sec urity in Local Area Networ k B ased on Fa st Encryption Algorithm", Internationa Journal of Comput ing Communicat ion and Information System (JCCIS) Journal Page 85-90. 2010.

[5] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evalua ting the E ffects of Symmetric Cryptogr aphy Algori thms on Power Consump tion for Diff erent Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept.

[6] Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Jour nal of Computer Sci ence and Communicati on Vol. 2, No. 1, January-June 2011, pp. 125-127

[7] Challa Narasimham, Jayaram Pradhan," EVALUATION OF PERFORMANCE CHARACTERISTICS OF CRYPTOSYS TEM USING TEXT FILES" Jo urnal of Theore tical and Applied Information Technology, pp55-59 2008.

[8] Abdel-Karim Al Tamimi," Perfo rmance Analysis of Data Encryption Algorithms "

[9] Prasithsangaree.P and Krishnamurthy.P (2003), "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the IEEE GLOBECOM 2003, pp. 1445-1449.

[10] Nidhi Singhal1, J.P.S.Raina2, Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology-July to Aug Issue 2011 pp177-181.

[11] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry," Efficiency and Security of Some Image Encryption Algorithms", Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

[12] Dr. S.A.M Rizvi1, Dr. Syed Zeeshan Hussain and Neeta Wadhwa" A Comparative Study Of Two Sy mmetric Encryption Algorit hms Acro ss Different Platforms",

[13] Turki Al-Somani, Khalid Al-Zamil "Performance Evaluation of Three Encryption/Decryption Algorithms on the SunOS and Linux Operating Systems", Theses

[14] Gurjeevan Singh, Ashwani Kumar Singla , K.S. Sandha," Th rough Put An alysis of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011

[15] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha" Through Put Analysis of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011.

[16] R.Chandramouli, "Battery power-aware encryption – ACM Transactions on Information and System Security (TISSEC),'' Vol. 9 Issue 2, May 2006.

[17] Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis of Encryp tion Algorithms For Da ta Commu nication", IJCST Vol. 2, Iss ue 2, June 2011 pp.192-192.

[18] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader 2, and Mohi y Mohamed Hadhoud2," Evaluating the Performance of Symme tric EncryptionAlgorithms", International Journal of Network Security, Vol.10, No.3, PP.213 {219, May 2010.

[19] Diaa Salama1, Hatem Abdual Kader2, and Mohiy Hadhoud2" Wireless Network Security Still has no Clothes", International Arab Journal of e-Technology, Vol. 2, No. 2, June 2011 pp.112-123.

[20]. N.Ruangchaijatupon and P. Krishnamurth "Encryption and power consumption in wireless LANs-N,"The Third IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, Sep. 27-28, 2001.

[21] Prasithsangaree.P and Krishnamurthy.P (2003), "Analysis of Ener gy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of theIEEE GLOBECOM 2003, pp. 1445-1449.

[22] Idrus.S.Z, Aljunid.S.A, Asi.S.M (2008), 'Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS Interna tional J ournal of Computer Science and Network Security, VOL.8 No.1, PP 20-25.

[23] Gast.M.S (2002),"802.11 Wireless Network: The Definitive Guide," O'REILLY.

[24] Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques" , International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.

[25] Ezedin Barka, Mohammed Boulmalf," On the Impact of Security on the Performance of WLANs", JOURNAL OF COMMUNICATIONS, VOL. 2, NO. 4, JUNE 2007, pp.10-17.

[26] D. S. Abdul. Elminaam et.al," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765, pp.58-64.

[27] Ramesh, G. Umarani, R., UMARAM: A novel fast encryption algorithm for data security in local area network http://ieeexplore.ieee.org /xpl/ freeabs_all.jsp? Arnumber=5670740

[28] G. Ramesh, R. Umarani," UR5: A Novel Symmetrical Encryption Algorithm with Fast Flexible and High S ecurity Based on Key Updation", European Journal of Scientific Research ISSN 1450-216X Vol.77 No.2 (2012), pp.275-292.

[29] Ramesh G, Umarani. R," UR5: A Novel Symmetrical Encryption Algorithm with Fast Flexible an d High S ecurity Based on Key Updation" , International Journal of Advanced Rese arch in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012 Page 16-22. 2010