Energizing the Advanced Encryption Standard (AES) for Better Performance

Arif Sari[1], Behnam Rahnama[2], Ibukun Eweoya[3] , Zafer Agdelen[4]
[1-4]Girne American University, Turkey, arifsari@gau.edu.tr,zagdelen@gau.edu.tr
[2]Scale DB. Inc. Silicon Valley, USA, behnam.rahnama@gmail.com
[3]Covenant University, Nigeria, ibukun.eweoya@covenantuniversity.edu.ng

Abstract— *Security is a never ending challenge. The security researchers must be steps ahead to avoid attacks and threats, thereby keeping businesses running and avoiding calamities. The Advanced Encryption Standard (AES) is to this rescue after its official acceptance and recommendation by National Institute of Standards and Technology (NIST) in 2001. However, timing attacks have called for a modification to it to retain its potency and effectiveness. This research boosts the Rijndael by incorporating an invented playfair ciphering into the algorithm using 256 ASCII codes. The concept counters possible leakages from the S-box lookups from the cache. The research introduces mixcolumn in the last round against the standard to make it a constant time algorithm. The encryption and decryption were validated. Previous researches implemented Architectural and operating system modifications, placing all the lookup tables in CPU registers, Parallel Field Programmable Gate Array (FPGA) implementation , Application Specific Integrated Circuits (ASIC) implementation, the Dynamic Cache Flushing Algorithm but none keeps AES assets of good speed and memory conservation; most especially in embedded systems.*

Index Terms— *AES, cryptanalysis, SCA, encryption, decryption, counter mode, security, FPGA, S-boxes.*

—————————— ◆ ——————————

1 Introduction

There is an unending list of cryptographic algorithms that have proved weak in one or all of authentication, authorization, logging, encryption, verification, validation or sanitization. According to [1], FIPS 140-2 defines a set of algorithms that have been determined to be strong. Symmetric keys less than 128 bits long are insecure, stream ciphers are discouraged due to subtle weaknesses. The NIST confirmed the AES excellent for usage in 2001, it is devoid of the above weaknesses [17]. However, it can be strengthened and that led to this research work.

The AES is in 128, 192 and 256 bits, we have strengthened further 256bits AES by an enhanced playfair cipher using ASCII implementation. The enhanced AES this paper presents is versatile and applicable in embedded systems, operating systems, web based applications, database applications etc. Hardware solutions require additional cost for simulation, control and monitoring equipment therefore the incoming of this research providing software solution presented by playfair ciphering with ASCII codes manipulations.

This research demonstrates the introduction of a unique diffusion and confusion in the Rijndael by incorporating playfair ciphering into the algorithm. It is dependent of the key and input, adding mixcolumns into the last round, thereby making it a constant time algorithm. The concept counters possible leakages from the S-box lookups, intermediary operations (addroundkey, substitutebyte, shiftrows, mixcolumns) of the AES are still applicable but it becomes impossible for cryptanalysis discovery of enciphering method; cracking efforts' success will be beyond human patience as it avoids statistical precision, thereby countering timing attacks.

Research Questions and Methodology.

The acceptability of AES is high and the efficiency is superb. However, lately challenges are eminent. Not much of attention was dedicated towards this in the past literature hence leading this research to some questions to bridge the gap?What is the vulnerability in AES?
What is the loop hole to cache timing attack ?
How can it be controlled?
The above questions have led us to a review of literature, shedding light on parameters that lead to AES vulnerability, exploring the loop holes to the attack and finally how to achieve a constant time algorithm, thereby bringing the cache timing attack to a halt.Using managed

————————————————

- [1-4]*Department of Management Information Systems,School of Applied Sciences,Girne American University, Cyprus asari@gau.edu.tr-zageleden@gau.edu.tr*
- [2]*ScaleDB Inc. Silicon Valley, USA behnam.rahnama@gmail.com*
- [3]*Department of Computer & Information Sciences, Covenant University, Ota, Nigeria. ibukun.eweoya@covenantuniversity.edu.ng*

code (.Net, Java, Php) was suggested by [2] to enhance security at the development stage of software development for their less susceptibility to overflow attacks and memory corruption therefore, php was chosen as the implementation language for this work.

According to [2], every sensitive information demands confidentiality, thereby avoiding loss, theft and corruption of data or information. The sensitivity of information in finance, health, defence, government etc. must be excellent in integrity, availability and confidentiality. The flow of data as required for any security conscious business is expressed in figure 1.

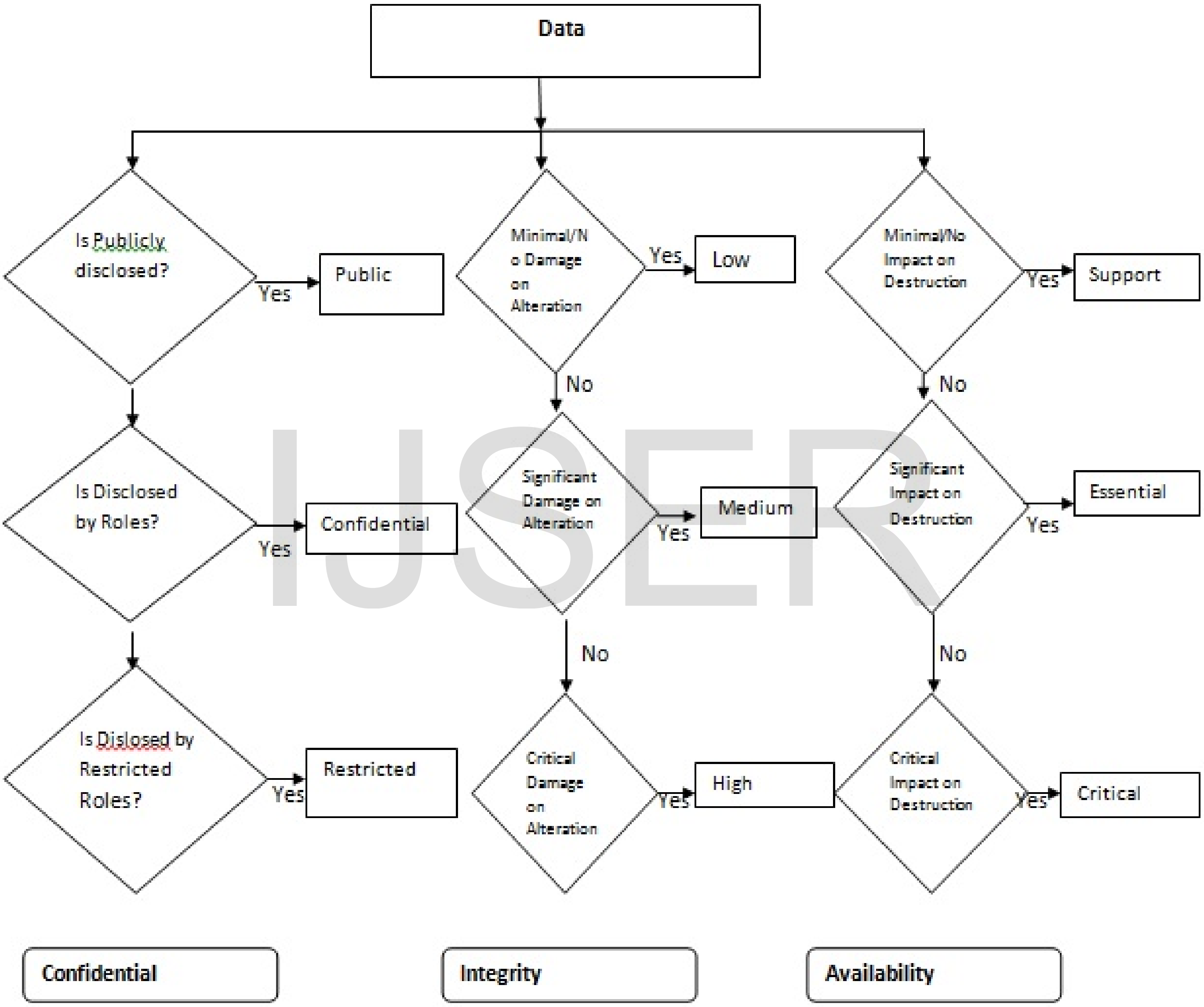

Data
Is Publicly disclosed?
Yes
Public
Is Disclosed by Roles?
Yes
Confidential
Is Dislosed by Restricted Roles?
Yes
Restricted
Minimal/No Damage on Alteration
Yes
Low
No
Significant Damage on Alteration
Yes
Medium
No
Critical Damage on Alteration
Yes
High
Minimal/No Impact on Destruction
Yes
Support
No
Significant Impact on Destruction
Yes
Essential
No
Critical Impact on Destruction
Yes
Critical
Confidential
Integrity
Availability

Figure 1: Example of a data classification flowchat [2]

2 Key Size and Encryption System

The ability to keep encrypted information secret is based not on the cryptographic algorithms which are widely known but on the key. The key must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple; decryption without the correct key is very difficult and impossible in some cases for all practical purposes [3].

The key size that should be used in a particular application of cryptography depends on two things: the key size, the cryptographic algorithm in use.

As each of these is of a different level of cryptographic complexity, it is usual to have different key sizes for the same level of security, depending upon the algorithm used. For example, the security available with a 1024-bit key using asymmetric RSA is considered approximately equal in security to an 80-bit key in a symmetric algorithm [4].

The following table compares the equivalent security level for some commonly considered key sizes [5].

Table Error! No text of specified style in document.**: Key Size Security Level Comparison [5]**

Comparison [5]

Symmetric scheme (key size in bits)	RSA(n in bits)	DLP (p in bits)	DLP (q in bits)	ECC (n in bits)
56	512	512	112	112
80	1024	1024	160	160
112	2048	2048	224	224
128	3072	3072	256	256
192	7680	7680	384	384
256	15360	15360	512	512

2.1 Losing and Compromising of Private Key

Considering a public key infrastructure (PKI), there is a high possibility of infringement of private keys. To avert key compromise consequences, there is a revocation of certificates linked to compromised keys. Despite the fact that the concerned certificates are still valid by expiry date specifications, they are confirmed irrelevant to dependants. The relying parties get informed about derailed certificates and consequently rendered invalid. Reasons accompany the Certificate Revocation List (CRL) or Online Certificate Status Protocol. Discretion comes into place about transactions done close to the arrival of the revocation alert [6] [7].

2.2 Confidentiality, Authentication, Integrity and Non – Repudiation

These are the important requirements for many cryptographic applications. A traditional approach to achieve these requirements is to signcrypt the message. Signcryption, first proposed by Zhang in 1997 [8] as a cryptographic primitive that performs digital signature and public key encryption simultaneously, at lower computational costs and communication overheads than the signature - then- encryption approach [9].

2.3 Information Confidentiality

Information means a set of data in an understandable form which contains some message. Information Confidentiality refers to the protection of a set of data or information from any unauthorized access. Data confidentiality and privacy are the foremost concerns in Information Confidentiality [10]. In the present age of networking (most significantly the internet), in a specific network, a certain piece of information is literally available everywhere within the network. Hence, Information Confidentiality becomes a serious issue, as taking any chance may result in information being leaked to unauthorized parties [11].

2.4 Integrity

Data integrity refers to the preservation of originality of information, simply preventing intentional compromise of data content. Integrity ensures that data hasn't been modified. Integrity is obviously extremely critical for any kind of transaction. Adulterated accounting or monetary documents can terminate businesses if not detected timely.

Hash algorithms are typically used to provide for integrity of information. A hash function is like the conventional fingerprinting, there is uniqueness in the item of information originality confirmation. If the data is modified, even a single bit changed, the fingerprint or hash is different, and the modification detected

2.5 Authentication and Non Repudiation

Authentication is an irrevocable capturing and consequently tallying of a personality or personalities in attempt to ensure there is no deviation from claimed identity. Identity cards, door locks and keys are for authentication purposes to gain entry. Network logins, passwords, access tokens, biometrics, watermarks and digital signatures are networking authentication measures.

Non repudiation refers to the inability of a person to deny the origin of a signature, document, and receipt of a message or document. An action taken cannot be revoked by a fraudulent personality and thereby causing a breach of security. This is observed in the verification and trust of signatures. Things pretended to be done under duress or boss instigation in official fraud then become legal issues in the court. Digital certificates are often based on the X.509V3 standard, and a Public Key Infrastructure (PKI) is employed.

3 The Hybrid Cryptography

There are several encryption schemes and each of them is specially steadfast for some unique application(s). Hash functions are inclined to data integrity. Secret key encryption is excellent for privacy and confidentiality.

In hybrid encryption, the sender can generate a session key on a per-message basis to encrypt the message; the receiver needs the same session key to decrypt the message. Key exchange is critical in public-key cryptography and can be used for non-repudiation and user authentication; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message.

Figure 2 is a three in one encryption called a hybrid cryptographic scheme; it possesses a secure transmission implementing digital signature and digital envelope.

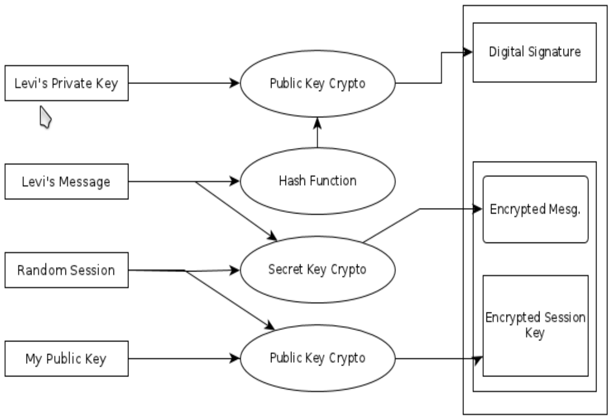


Figure 2: Sample Application of the Three Cryptographic Techniques for Secure Communication [10].

A digital envelope is a product of enciphered information and session key. The session key is randomly generated. The recepient's public key being enciphered by the sender in the session key. The recepient's secret key gives the session's secret key and the product is a digital envelope.

3.1 Digital Signature

The digital signature describes an asymmetric encryption process to warranty the authenticity and integrity of electronic data and to check a user's identity. In most cases it conforms to a handwritten signature or may be compared with a means of clearly proving one's identity (identity card). The legal effect of a digital signature in Germany is regulated by the Digital Signature Act [12].

Forging digital signature is difficult unlike manual signatures. Digital signature schemes are cryptographically based, effectiveness is achieved by a carefully planned and executed encryption. There is a hash value computation, encryption and decryption to give the exact hash value to the recipient hence, a confirmation of no alteration of information on transit.

3.2 Cryptographic Techniques

The basic building blocks of cryptographic applications and protocols are the cryptographic algorithms. This section summarizes most of the important encryption algorithms including hash functions, stream ciphers, and other basic cryptographic algorithms. RSA (Rivest, Shamir and Adleman) is probably the most widely used public key cryptosystem; it uses large prime numbers to construct the key pairs. The Data Encryption Algorithm (DEA) has a 64-bit block size and uses a 56-bit key during execution (8 parity bits are stripped off from the full 64-bit key). The DEA is a symmetric cryptosystem, specifically a 16-round Feistel cipher. Digital Signature algorithm, elliptic curve cryptosystems, RC2 and RC4, RC5 and RC6 (Rivest's cipher or Ron's code.) Secure hash algorithm and message digest algorithms are some of the cryptographic techniques of high relevance [13].

4 Advanced Encryption Standard Analysis

The standard comprises three block ciphers, AES -128, AES-192, and AES 256, adopted from a larger collection originally published as Rijndael. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192, and 256 bits respectively. The AES ciphers have been analyzed extensively and are now used worldwide as was the case of the Data Encryption Standard[14]. The Counter mode can be used by the wireless body area networks (BNs) to encrypt data [10].

The Rijndael cipher was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen and substituted by them to the AES selection process [15]. The AES is a standard block cipher. It encrypts and decrypts data with a secret key and not two as found in DES, using substitution and permutation concepts namely: SubBytes, ShiftRows, MixColumns and AddRoundkey over many rounds (10 for a 128-bit key). A common optimization technique on 32-bit processors is to precompute series of tables on the basis of the combination of these primitives. AES encryption then becomes a series of table lookups and XOR operations [16].

Both in encryption and decryption process, the state array is modified at each round by a round function that defines four different byte-oriented transformations [17], [18]. SubBytes transformation, ShiftRows transformation, MixColumns, AddRoundKey, these four are expatiated at the implementation stage of this thesis.

Because the index for these AES tables is the XOR of a plaintext byte and a key byte, the indices themselves must remain secret. However, a spy process running on the same system can observe the variable timing of the AES encryption due to cache behaviour, narrowing down the possible values for the key [19].

According to[20] [21], the AES encryption itself takes only 11 cycles, but the complete program with loading the data and key, AES encryption, and returning the result back to the software routine takes a total of 704 cycles. AES-Rijndael decryption was found to consume approximately up to 20-30% more energy than encryption. Nevertheless, its performance is very good and seems likely to remain so since it uses only efficient and commonly available instructions.

The surprising growth of the internet and the fiery growth in computer networks have increased the dependence of both organizations and individuals on the information stored and disseminated by these systems. However, at the same time it also brought about a plethora of new issues and concerns, the utmost among them being the need to protect data and resources from disclosure, guarantying the authenticity of data and messages, also protecting systems from network based attacks [13].

The amount of computational energy consumed by cryptographic algorithms on a given microprocessor is proportional to the number of clocks needed by the processor to compute the cryptographic algorithm. There have been some studies about the energy efficiency of encryption algorithms for wireless devices [22].

5 Digital Certificates and Key Management

A certificate is a data structure that includes an entity's name along with any information that is to be bound to that name. The entire certificate is signed by a Certificate Authority (CA). In order to be effective, the CA's public key must be well known (or be available through some secure mechanism) and the CA must be widely trusted. The use of certificates is complicated by the possibility that information in the certificate will change. In order to enhance security, entities periodically change their public keys.

In addition, people may change their names, jobs, or job titles. If a certificate contains attributes that are no longer valid, then the certificate should no longer be considered valid. As a general rule, entities change their public keys on a regular schedule. In order to support this in a clean manner, most certificates include expiration dates. The expiration date represents the time after which the CA that created the certificate is no longer willing to claim that the information contained in the certificate is valid.

Unlike the regularly scheduled change of public keys, name and job changes cannot always be predicted far enough in advance to set the expiration dates on certificates correctly (certificates are frequently valid for a year or longer) [6], [7]. Of even more concern, a user's private key may be compromised. A private key is considered to be compromised whenever it is in the possession of someone other than the key's owner (or someone trusted by the key's owner). Once a user's private key has been compromised, any certificate containing the corresponding public key should be revoked.

In order for CAs to invalidate (i.e., revoke) certificates before they expire, CAs must have some mechanism for distributing certificate status information. The two most common mechanisms for disseminating this information to relying parties are certificate revocation lists (CRLs) and on-line certificate status protocols (OCSP).

The keys in use are critical to the cryptographic security process, keeping it from intruders and bringing in some concepts to ascertain its authenticity enhances the reliability of the encryption method in use.

6 Description of AES Algorithm and Modifications

1. KeyExpansion- Rijndael's key schedule to get round keys from the cipker key
2. Initial Round – Implements addroundkey combining each state byte with the round key employing XOR.
3. Rounds

    1. SubBytes - The code generated s-box is used here for a non linear substitution of bytes

    2. ShiftRows - All rows except the first are shifted cyclically a certain number of steps as a transposition for enhanced diffusion.

    3. MixColumns - A mixing operation which operates on the columns of the state, combining the four bytes in each column.

    4. AddRoundKey

4. Final Round (no MixColumns)

    1. SubBytes

    2. ShiftRows

    3. AddRoundKey

Motivated by the work in [23], [24], [25], evaluation of a block cipher computational complexity and energy consumption is a function of basic operations required to achieve a comit and not a rollback of the planned algorithm.

Many iterations and operations are involved in the encryption and decryption process depending on the size of the cipher key where each round performs some specific functions. The scramling and unscrambling of 128 bit cipher key entails 10 different rounds for an absolute process execution [26]. For encryption or decryption, each round (called the round function) of AES (except the last round) consists of four stages [27]. Figure 3 explores AES-128 algorithm

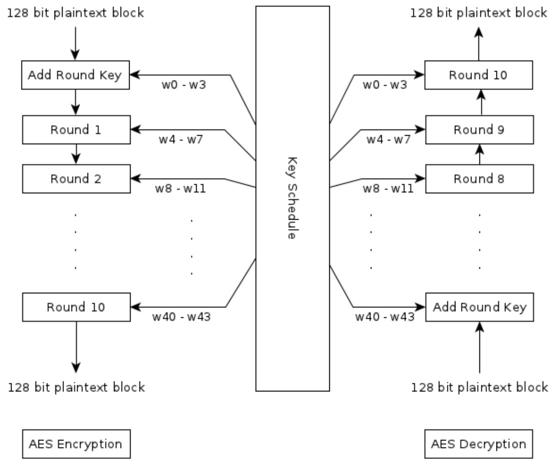


Figure 3: AES -128 Flow Diagram [13].

6.1 Applications

The veteran security capability and topmost efficiency of AES make it suitable in solving security problems in the accounting information systems in storage, information exchange, security subsystem and also the birth of fresh comprehensive account systems for e- business.

According to [28], the security threats in the accounting system are reliably resolved by AES algorithm.

Multimedia data is humanly explored constantly therefore image encryption is paramount for memory preservation and pixels security in transmission over networks. There is a proposed scheme which combines Discrete Wavelet Transform (DWT), Embedded ZeroTree Wavelet algorithm (EZT) and the AES to effect security of stream(AES) and reduce total amount of data by compression (DWT and EZT).

Despite NIST's hype of the AES, according to latest researches in [9], for the state of the art embedded systems and real time systems, software AES cipher capability speed effectiveness has a shortfall for encryption to be incorporated ubiquitously for computational requirements. However, the AES version that is more speed compliant uses table lookups and are susceptible to software cache-based side channel attacks, leaking the secret encryption key [9]. To bridge the gap between software and hardware AES implementations, several Instruction Set Architecture (ISA) extensions have been proposed to provide a speed up for software AES programs, most notably the recent introduction of six AES-specific instructions for Intel microprocessors. However, algorithm-specific instructions are less desirable than general-purpose ones for microprocessors [9]. As the performance of microprocessors improves, the performance of software AES encryption and decryption also improves.

It is no news anymore that wireless channels are vulnerable to security attacks, so is WBAN though still fresh in its researches vulnerable to eavesdropping, data modification, impersonation, replaying and denial of service.

The detail security requirements of WBAN are introduced in [29]. Patients' private biomedical data deserves privacy thereby data encryption, data integrity, authentication, freshness protection and denial of service (DoS) detection are WBAN security services and AES can be part of the hybrid security mechanism used for the encryption. The AES code size (single key requirement as a symmetric key algorithm), processing time and power or energy consumption qualifies it for the task. The existing security provisions for Wireless Security Network (WSN) generality do not suit WBAN due to resource restrictions and application types [30] [31].

6.2 Security Strength of AES

The 128 bits key length is the least key size, implying 2^{128} brute force attempts. Performing exhaustive search in this huge key space is considered infeasible. Thus the brute-force attack against AES with current and projected technology is considered impractical.

AES uses s-box substitution table which is generated by determining the multiplicative inverse for a given number in Galois finite field and has the capability to resist the linear and differential cryptanalysis. According to [26], a hacker can easily attack a variable time AES algorithm and can crack the encrypted data and eventually key through a cache timing attack.

Recently Warren D. Smith has defined an analytical method and claimed that there is a possibility of existence of a cracking algorithm that will be able to extract the AES 256 bits key from any random plaintext- ciphertext pairs [32], [18]. However, he enjoyed his freedom of opinion as no cracking algorithm was provided for a proof. Obviously, AES algorithm doesn't have any mathematical property that can be exploited by an attacker to reduce the effective key length and to gain success against AES.

The FPGA implementation of AES encryption and decryption uses VHDL for hardware description, Xilinx – Project Navigator, ISE 8.2i suite for software while simulation tools in ModelSim SE PLUS 5.7g are employed for the simulation [33].

7 Suggested Remedy to AES Cache Timing Attack

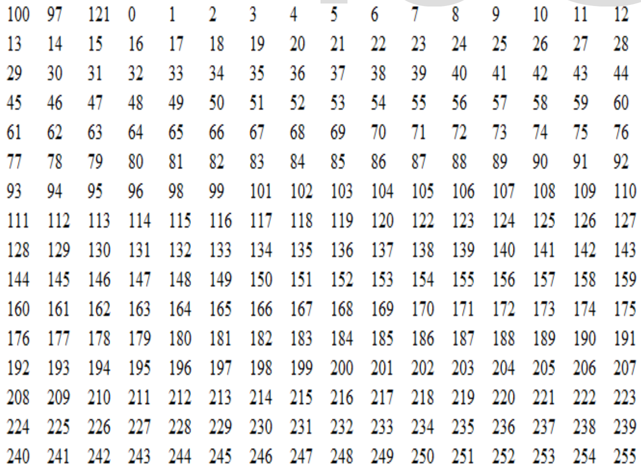
A key is chosen by the user, the program converts the key to their ASCII codes. A one dimensional array stores the ASCII values of the key and later they are the first in a two dimensional array of 16 by 16. Filling up the 256 uniquely and key dependent generated array, no ASCII value of the key member is repeated. The elements to be encrypted are treated in pairs, when the pair is on the same row, a left shift is done once and the last on the row falls back on the first. A pair on the same column entails a downward shift and the last on the column falls back on the first on the column. The pair on different row and different column is replaced by diagonal ASCII values for the encryption.

The actual 128bits block length and 256bits key length data or information undergo the AES encryption and then playfair encrypted after the substitution and permutation by addroundkey, subbytes, shiftrows, mixcolumn and subsequently decryption. Finally, there are 14 rounds of playfair insertion into an equivalent rounds of Rijndael, mixcolumns is included in the last round in this research. This averts the cache timing attack as variables arrive at the cache at a constant time and tapping timing differences from the cache for cryptanalysis by attackers is prevented, thereby countering the vulnerability of AES to cache timing attacks which is the focus of the work. The hardware

Playfair is the best known multiple-letter cipher. Playfair is based on a 5 x 5 matrix of letters constructed based on a keyword that is chosen by a user. Lord Peter Wimsey provides an example [13].

The traditional playfair cipher consists of 26 characters (upper case) of the alphabetical series, the author modified playfair cipher to contain 256 characters in the 16 x 16 array thereby allowing the contents of the ASCII table to be saved in the array for encryption thus providing a wider range of character and symbols for better encryption of text.

Encryption in playfair is done based on substitution. Playfair encrypts the contents of the array two elements at a time.



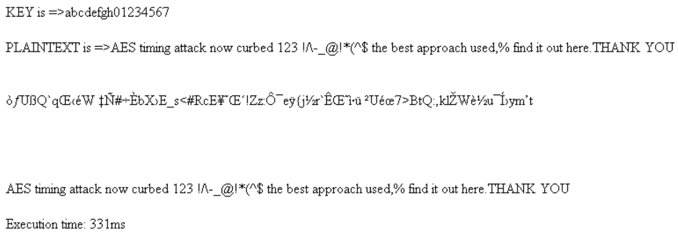
100	97	121	0	1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92
93	94	95	96	98	99	101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Figure 5: Modified playfair using daddy as the key

Conclusion and Future Work

The playfair cipher was a powerful tool during World War II but nearing extinction. This work turns the traditional playfair of 26characters substitution into 256 ASCII codes substitution and permutation. The author incorporates this into the AES encryption and modified that by introducing mixcolumn into the last round of AES.

configuration of the computer in use is a factor in the execution speed in microseconds. The screenshot below is the output of the validation.



```
KEY is =>abcdefgh01234567

PLAINTEXT is =>AES timing attack now curbed 123 !^-_@!*(^$ the best approach used,% find it out here.THANK YOU

ð ƒUßQ`qŒ‹éW ‡Ñ#÷ÈbX›E_s<#RcE¥˘Œ'!Zz:Ô¯eÿ{j½r`ÊŒ˜i·ü ²Uéœ7>BtQ:,klŽWè½u¯Í›ym't



AES timing attack now curbed 123 !^-_@!*(^$ the best approach used,% find it out here.THANK YOU

Execution time: 331ms
```

Figure 4: A screenshot of the output

Plaintext letters that fall on the same row matrix are each replaced by the right, with the first element of the row circularly following the last. The plaintext letters that fall on the same column are replaced by the one directly below them or the one at the beginning of the column in case of a letter in the last row. In a case where both conditions are not satisfied, the diagonal of letters are used to replace the plaintext. Repetition of characters are neglected, hence daddy is treated as day, neglecting the middle ds. Figure 5 gives an expression of the above. 100, 97, 121 are ASCII codes for d, a and y respectively.

REFERENCES

The hardware development along this path using the developed software could be a worthy investment to ascertain its speed on embedded systems by FPGA,VDHL or ASIC.

The key length could be increased beyond 256bits in the future as nobody knows what tomorrow holds hence the conjecture.

Conflict of Interest

The author(s) declare(s) that there is no conflict of interests regarding the publication of this manuscript.

[1] Simpson et al. (2008), Fundamental Practices for Secure Software Development, A Guide to the Most Effective Secure Development Practices in Use Today, available at: www.safecode.org/publications/SAFECode_Dev_Practices1108.pdf

[2] Mano P. (2012), The Ten Best Practices for Secure Software Development, available at: www.isc2.org/uploadedFiles/(ISC)2_Public.../ISC2_WPIV.pdf

[3] Amoroso, E.(1994) Fundamentals of Computer Security Technology, New York: Prentice Hall.

[4] Rivest, R., Shamir, A., Adleman, L. (2000). Official RSA publication on e-commerce.

[5] http://www.nsa.gov/business/programs/elliptic_curve.shtml

[6] Housley, R., Ford, W, Polk, W. and Solo, D. (1998) Internet x.509 Public Key Infrastructure Certificate and CRL Pole. IETF X.509 PKI (PKIX) Working group, (draft).

[7] Myers, M., Ankney, R., Malpani, A., Galperin, S. and Adams, C. (2007). X.509 Internet Public key Infrastructure Online Certificates.

[8] Nuckolls, G. (2005). Verified Query Results from Hybrid authentication Trees. Processing of Database Security, 84-98.