International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Digital Signature based on Elliptic Curve Cryptography and Playfair Cipher

Anagha G[1], Prof. Smitha GR[2]

[1]Student, Dept. of Information Science and Engineering,R.V. College of Engineering, Bengaluru, India
[2] Assistant Professor, Dept. of Information Science and Engineering, R.V. College of Engineering, Bengaluru, India

---

Abstract - *The exchange of information and data over unsecured networks is vulnerable to data stealing and attacking, which necessitates the study of Cryptography. Cryptography is the technique of protecting information and communication by the use of codes, so that it can only be interpreted and processed by those for whom the information is intended. A digital signature which is a cryptographic technique to authentication and data integrity uses mathematical operations to find the signature and relies on the message being sent and the sender. It is also known as digital footprint. Unlike manual signatures, the digital signature changes with messages. In this paper, a new digital signature scheme technique is proposed that combines Elliptic Curve Cryptosystem and extended Playfair cipher. This scheme can be used for digital signature. The proposed method is compared with the existing Elliptic Curve Digital Signature Algorithm to understand the performance during signature and verification process. The results are found to be comparable in terms of time taken. In terms of security, the new scheme adds data confidentiality by using extended Playfair cipher.*

Key Words: Cryptography, Digital Signatures, Elliptic Curve Cryptography, Playfair Cipher, Authentication, Extended Playfair Cipher, ECDSA

1.INTRODUCTION

As the use of digital data increases, the necessity to provide security against newly emerging attack techniques everyday becomes obvious. Cryptography is a branch of science that discusses various mathematical techniques to maintain data security. At times, the digital data not just requires the confidentiality maintained but also the authenticity of the data source should be ensured. Digital Signature is an approach in this regard that can be used to provide authenticity, data integrity and non-repudiation [8]. It is a digital counterpart of traditional signatures except that it uses the data along with a key that is private to the sender. Many research works are under progress with respect digital signatures. A technique call Playgamal Cipher Algorithm[1] is proposed. This combines the Elgamal algorithm with Playfair cipher and is compares with traditional Elgamal encryption scheme. The results show that Playgamal can be used in place of Elgamal as there is no performance degradation. Also, further studies to evaluate the strength of this scheme in real case are yet to be made.

A new scheme of digital signature is discussed by combining Elliptic Curve Cryptography (ECC) with Ong, Schnorr and Shamir(OSS) scheme [2]. It uses a 4x4 self invertible key matrix for OSS signature equations. This increases the overall security as well as performance since the key matrix is self-invertible and can be used for both encryption and decryption. Similar scheme was also proposed by for image encryption using Elliptic Curve Cryptosystem with Hill Cipher (ECCHC) [3].

Another scheme using DNA encryption/decryption was proposed and this is similar to Playgamal proposed in [1] except that the Playfair cipher is replaced with DNA techniques.

A comparison of ECDSA with RSA based Digital signature is drawn [5] where a detailed analysis of key generation time and signature generation time is made for both the algorithms. ECC provides same security with less key size when compared to RSA and is preferred over RSA. A review is given in various aspects including time, security and power.

A new ECDSA is proposed [6] which does not involve a lot of point operations as in existing ECDSA. It shares only two points in contrast to three points when existing ECDSA is considered.

An extended Playfair cipher algorithm[7] is proposed to address the drawbacks of 5x5 key matrix are outlined and in order to overcome them, 8x8 matrix is used. The cipher is tested against cryptanalysis and avalanche effect which shows that extended Playfair cipher is stronger. Another cipher technique for making playfair cipher is proposed [10] where 7x7 matrix is created by using indexing and filling the matrix with different patterns like spiral configuration, J configuration and diagonal.

When compared to various schemes, ECDSA gains more importance as this is faster and lighter. It can be used in wide range of applications. This research is an attempt to combine these algorithms that would result in a signature scheme

that provides both the benefits of confidentiality and authenticity.

2. PROPOSED SCHEME

The proposed scheme can be divided into two parts: Sender and Receiver. The message to be sent is encrypted using extended playfair cipher. Then, the message digest is created using the hash algorithm and in this implementation the hash algorithm used is SHA256. The sender creates the signature using his private key of the key pair by encrypting using ECDSA. Fig - 1 shows the flow chart for the sender side.

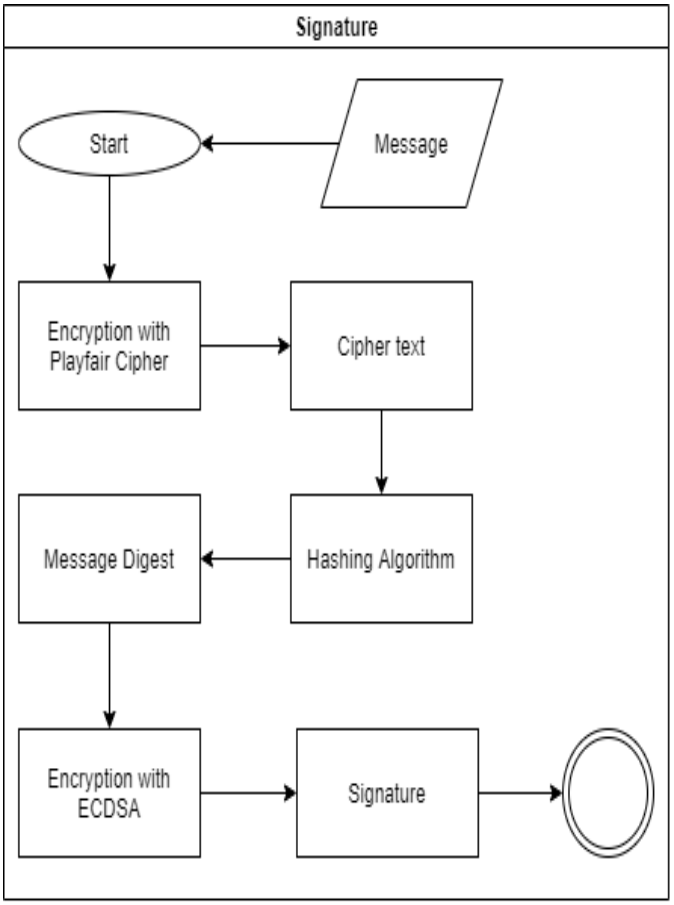

Fig -1: Sender's Side

On the receiver end as shown in Fig - 2, the message in the encrypted form is first applied hash function. This hash value is then compared with the result obtained from decrypting the signature with ECDSA technique. Ideally, these values should be same to confirm that the signature is verified. Only when the verification is successful, the decryption of the message received is done. To ensure that the decryption is not applied by an attacker without verification step, the key for Playfair cipher is computed from a secret key shared independently of the sending steps described before.

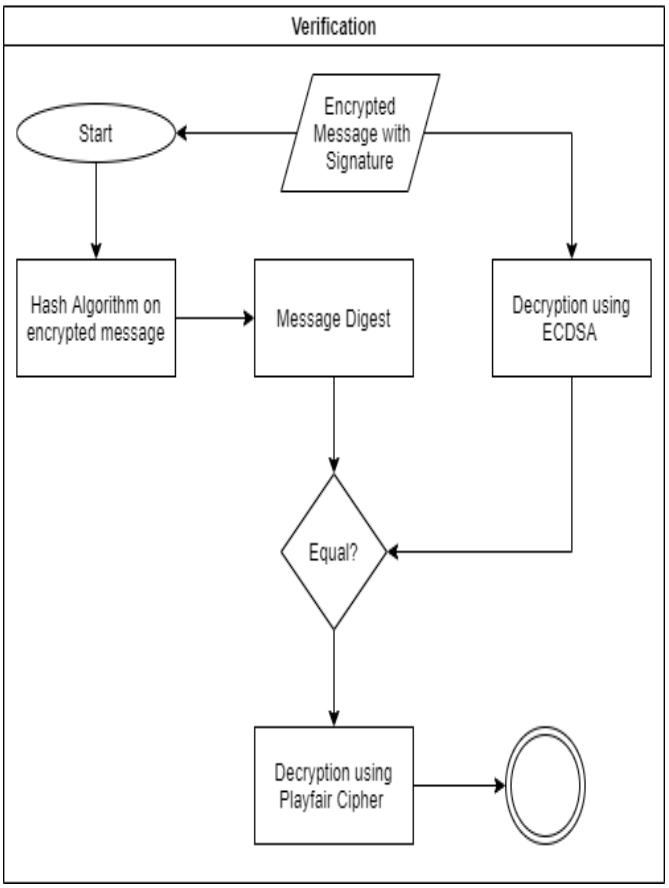

Fig -2: Receiver's Side

2.1 Extended Playfair Cipher

Playfair cipher is a symmetric algorithm and was developed by a British physicist Sir Charles Wheatstone. Playfair cipher uses a 5 x 5 key matrix which is shown in Table-1. It requires a keyword for the construction of the matrix arranging the 25 alphabet eliminating J. However the size of the matrix is not a standard rule [7] and it can be modified to be able to support other characters as well.

Table -1: 5X5 key matrix for keyword = 'KEYWORD'

K	E	Y	W	O
R	D	A	B	C
F	G	H	I	L
M	N	P	Q	S
T	U	V	X	Z

In the extended playfair cipher, 8x8 matrix is constructed and the encryption can be applied to alphabets, numerals and special characters. Table-2 shows 8x8 matrix. "|" is used in place of space and "^" is used for padding in case repeated character is encountered as well as when the total length is odd in number. While decryption, "|" is replaced with a blank

space and "^" is discarded. The rules for encryption remain same. The message is encrypted in digrams. With the use of 8x8 matrix, the number of digrams increases to 4096 which makes cryptanalysis difficult.

The formation of the Playfair key matrix requires a keyword. This keyword is generated using a random number generated and MD5 is applied after which the byte array is converted to ASCII characters. This is used as keyword in generating the key matrix.

Table -2: 8X8 key matrix for keyword = 'KEYWORD'

K	E	Y	W	O	R	D	A
B	C	F	G	H	I	J	L
M	N	P	Q	S	T	U	V
X	Z	0	1	2	3	4	5
6	7	8	9	!	@	#	$
%	^	&	*	(	)	_	+
=	{	}	[	]	\	|	:
;	'	,	<	>	/	.	?

2.2 ECDSA

Elliptic Curve Cryptography is gaining importance as it provides high security with smaller key sizes, less computation and less memory usage. It is now used in wide range of applications like embedded systems, portable devices and mobile devices.

Elliptic Curve Operations are used in signing process. The major operations are Point Addition and Point Multiplication. Point Multiplication is nothing but repeated self addition and a scalar is provided. Fig - 3 and Fig - 4 show the point operations on elliptic curve.

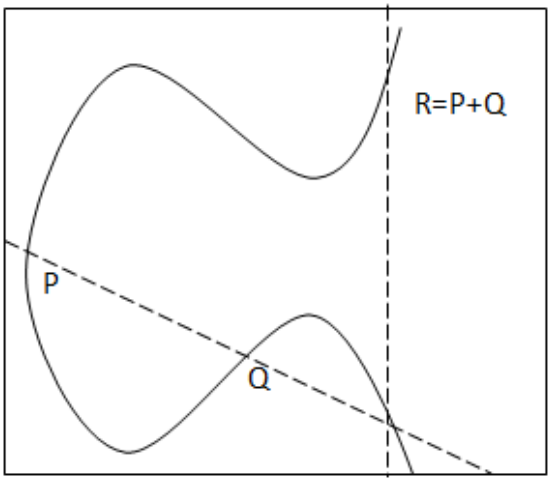

Fig -3: Point Addition Operation

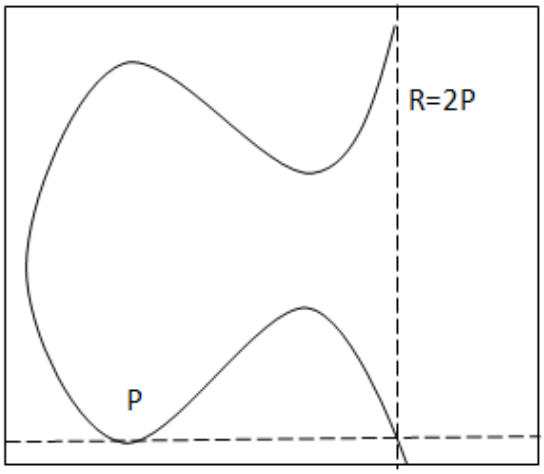

Fig -4: Point Multiplication Operation

Key Generation –

A key pair for a user is created and is associated to a set of Elliptic Curve domain parameters $D= (q,FR,a,b,G,n,h)$ where

E is an elliptic curve over Fq,
P is prime order point,
FR is Field Representation and indicates the representation used for elements in Fq.
a and b are field elements and define the equation of the elliptic curve E.
G is a point of prime order in $E(Fq)$. h is the co-factor $/E(Fq)//n$.

Key generation requires the selection of a random integer d in $[1,n-1]$. The public key is calculated as $Q=dP$ and d is the private key.

Signature Generation –

A random integer k is selected in the interval $[1,n-1]$.
$kP=x1,y1$ is determined.
$r=x1 \bmod n$ is calculated and if found to be 0, k is chosen again. Else, $k^{-1} \bmod n$ is computed.

Next, $s= k\text{-}1 \{h(m)+ dr\} \bmod n$ is determined, where h is the Hash Algorithm. If $s = 0$, the generation is started all over again. Else, the signature for the message m is (r,s)

Signature Verification –

When the receiver gets the message and signature, the verification begins with checking if r and s are integers in $[1,n-1]$.

Then $w = s\text{-}1 \bmod n$ and $h(m)$ is computed which is used in calculating $u1$ and $u2$ as:

$u1 = h(m)w \bmod n$
$u2 = rw \bmod n.$

The next step is to calculate *u1P + u2Q =(x0,y0)* and *v= x0 mod n*. If *v = r*, the signature is verified.

4. RESULTS AND DISCUSSION

The proposed algorithm was implemented on a system with i5 processor and 8 GB RAM. The performance results of running time are compared with the running time of ECDSA. The running times for both the algorithms are found to be comparable when the input size is not too large. Fig - 5 summarizes these results. The values in the chart are average and are found by applying the algorithm for each case multiple times to find the aggregate.

The new scheme is found to have extra security as it involves encryption before signature. During verifying the message is obtained to the receiver only if the signature is verified. Also, it can be accessed by the intended receiver only as the key is kept secret and shared before.

Playfair cipher uses 8x8 matrix and is able to encode meaningful sentences with alphanumeric values and special characters. To make the cipher more secure against cryptanalysis, the playfair cipher algorithm can be modified to introduce confusion so that the frequency information of alphabet cannot be used by an attacker to get the original message.

Extended playfair cipher still lacks some of the characters and can be applied only to a limited alphabet set. Also, the performance with respect to encrypt/decrypt time is less when the input size is significantly large. The playfair cipher could be modified and tested to run in parallel threads as a next step.

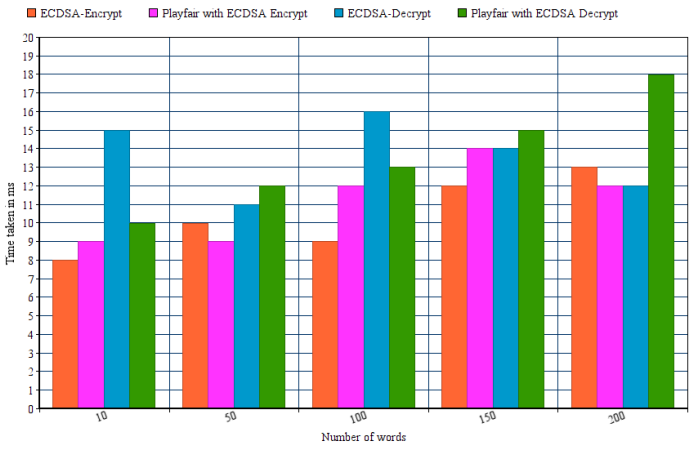

Fig -5: Comparison of ECDSA with new scheme

4. CONCLUSIONS

Cryptographic algorithms provide data security and authenticity. Digital Signatures are cryptographic solutions to achieve integrity, authenticity and non-repudiation. Various schemes for Digital signatures are discussed. A new scheme is proposed that combines ECC and extended playfair cipher. This has resulted in achieving confidentiality while sharing messages. Also, the encryption-decryption times are comparable with ECDSA. However, the performance may degrade as the input size increases and in the future, the scheme has to be tested for various applications and optimized accordingly.

REFERENCES

[1] A. Ghofar, M. Hardi, M. N. Firdaus and G. F. Shidik, "Digital signature based on PlayGamal algorithm," 2017 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, 2017, pp. 58-65.

[2] H. M. Elkamchouchi, A. E. Takieldeen and M. A. Shawky, "An advanced hybrid technique for digital signature scheme," 2018 5th International Conference on Electrical and Electronic Engineering (ICEEE), Istanbul, 2018, pp. 375-379.

[3] Dawahdeh, Ziad & Yaakob, Shahrul & Othman, Rozmie Razif. (2017). A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher. Journal of King Saud University - Computer and Information Sciences. 30. 10.1016/j.jksuci.2017.06.004.

[4] R. Kasodhan and N. Gupta, "A New Approach of Digital Signature Verification based on BioGamal Algorithm," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2019, pp. 10-15.

[5] D. Toradmalle, R. Singh, H. Shastri, N. Naik and V. Panchidi, "Prominence Of ECDSA Over RSA Digital Signature Algorithm," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, India, 2018, pp. 253-257.

[6] S. Lamba and M. Sharma, "An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA)," 2013 International Conference on Machine Intelligence and Research Advancement, Katra, 2013, pp. 179-183.

[7] Srivastava, Shiv & Gupta, Nitin. (2011). A Novel Approach to Security using Extended Playfair Cipher. International Journal of Computer Applications. 20. 10.5120/2435-3276.

[8] R. Kaur and A. Kaur, "Digital Signature," 2012 International Conference on Computing Sciences, Phagwara, 2012, pp. 295-301.

[9] Roy, Dr. Abhishek & Karforma, Sunil. (2012). A survey on digital signatures and its applications. JCIT. 3. 45-69.

[10] Shakil, Tahmid & Islam, Md. (2014). An Efficient Modification to Playfair Cipher. ULAB Journal of Science and Engineering. 5. 26.