PLAYFAIR CIPHER 10*9

Introduction

The study of mathematical methods pertaining to information security elements like entity authentication, data integrity, confidentiality, and data origin authentication is known as cryptography. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications. Encryption is one of the techniques that are discussed. One Interacting with data and information through a variety of communication channels is one of its basic uses. Not all these channels are reliable. To ensure confidentiality, information or data must be hidden before communication begins. Encryption is the process of hiding data before sending it over a communication channel, though its goals can vary. Most of the cryptosystem uses a general framework to encrypt and decrypt data. There are several components involved, including plaintext, ciphertext, encryption, decryption, and key. (Shakil, 2015)

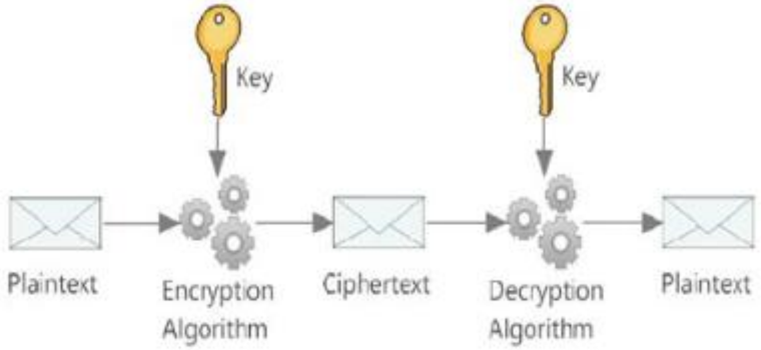


Figure 1 General structure of cryptography. (Islam, 2014)

Security:

Security, in a broad sense, refers to the protection of assets or systems from various threats, risks, and unauthorized access. The concept of security can be applied to different domains, including information security, computer security, network security, physical security, and more. (nikitawootten, 2023)

CIA:

By guaranteeing authorized access (Confidentiality), preserving accuracy (Integrity) by preventing unauthorized changes, and guaranteeing continuous accessibility (Availability) with safeguards against disruptions, the CIA Triad principles work together to protect information. These guidelines serve as the cornerstone of a robust security posture, protecting maintaining accuracy, protecting sensitive data, and guaranteeing authorized user access. (Franklin, 2023)

Figure= https://www.cia.gov/

History of Cryptography:

In this modern day of information and technology, we sometimes take for granted the complex mathematics and tools that allow us to send sensitive data all over the world without worrying about breaches in confidentiality or integrity. The act of encoding and decoding information has a long and complex history dating all the way back to ancient Rome and Egypt. For thousands of years, humans have been inventing increasingly complex information-hiding schemes, and other humans have been breaking them. We've gone from very simple encodings that rely on a simple secret shared between parties to incredibly complex computer algorithms that are publicly known yet still secure and rely only on the computational complexity bounds of the underlying mathematics as we understand them today. (Timour, 2023). There are three eras in the history of cryptography,

- (Ancient era)Manual era: Manual era refers to Pen and paper Cryptography and dates to 2000 B.C. e.g., Scytale, Atbash, Caesar and Vigenère.
- Mechanical era: Mechanical era refers to the invention of cipher machines. E.g.: Japanese Red and purple machine, German Enigma. Modern era of cryptography
- Modern era: Modern era of cryptography refers to computers. They are infinity permutations of cryptography available using computers. E.g.: Lucifer, Rijndael, RSA, ELGamal.

Classic cryptography:

It is said that the Greeks of classical antiquity were familiar with ciphers, such as the scytale transposition cipher, which is said to have been employed by the Spartan military. Steganography was also created in antiquity; it is the practice of concealing even the existence of a message to maintain its confidentiality. An early instance, described by Herodotus, involved a tattoo of a message hidden beneath the growing hair on a slave's shaved head. The use of digital watermarks, invisible ink, and microdots to hide information are more recent instances of steganography. A classical cipher's (and some modern ciphers') ciphertexts will reveal statistical information about the plaintext, and this information is frequently exploitable to crack the cipher. After the discovery of frequency analysis, perhaps by the Arab mathematician and polymath Al-Kindi (also known as Alkindus) in the 9th century, nearly all such ciphers could be broken by an informed attacker. Even now, people still find these old-fashioned ciphers entertaining, albeit mostly as riddles (see cryptogram). In his book (alMu'amma, 1992) (Manuscript for the Deciphering Cryptographic Messages), Al-Kindi wrote about the first known application of frequency analysis. Methods of cryptanalysis (S.P, 2017)

First page of a book by Al-Kindi which discusses encryption of messages

Figure from: https://www.samieltamawy.com/the-arab-cryptanalysts-and-al-kindis-methods/

Computer era:

The post-World War II era saw a profound transformation in cryptography with the advent of digital computers. This technological leap enabled the development of more intricate ciphers and expanded encryption capabilities to encompass diverse binary data, surpassing the limitations of classical ciphers designed for written language texts. While computers facilitated both the design of sophisticated ciphers and advancements in cryptanalysis, modern ciphers have effectively outpaced decryption efforts due to their efficiency and computational complexity.

Academic research in cryptography gained momentum in the mid-1970s, resulting in milestones such as IBM's Federal Data Encryption Standard algorithm, Whitfield Diffie and Martin Hellman's key agreement algorithm, and the RSA algorithm. Cryptography has become an indispensable tool in communications, computer networks, and overall security. Designers now grapple with anticipating future developments, considering factors like the continuous enhancement of computer processing power and the looming impact of quantum computing, as they work to ensure the resilience and effectiveness of cryptographic systems. (Sababa, 2018)

German Lorenz cipher, used in world war II to encrypt very high level general staff messages.

Fig: https://www.slideshare.net/EmaSushan/cryptography-232430021

Types of Cryptography:

Based on how the system performs encryption and decryption, there are essentially two types of cryptosystems:

- Symmetric Key encryption
- Asymmetric Key encryption

The link between the encryption and the decryption key is the primary distinction between various cryptosystems. It makes sense that both keys are tightly related in any cryptosystem. Using a key unrelated to the encryption key to decrypt the ciphertext is nearly impossible.

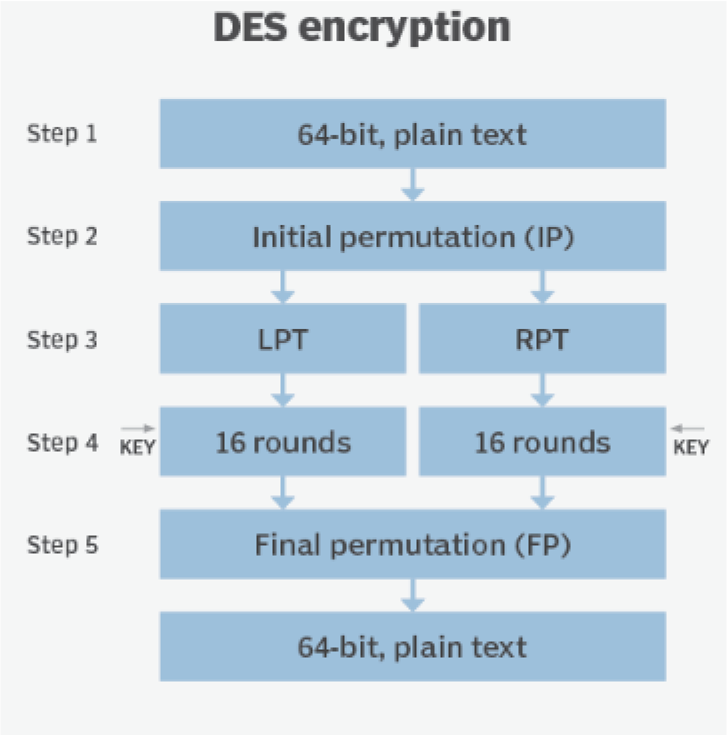
Symmetric Key encryption:

Symmetric key encryption is faster than asymmetric encryption because each user of the encryption system has a copy of the single secret key that is used for both encryption and decryption. In symmetric encryption, the sender and the recipient share the same secret key, which is used for the decryption process. It becomes dangerous to utilize the secret key since both the sender and the recipient have access to it. It is advised to utilize symmetric key encryption with a greater key length of 128 bits to prevent or make any attempt at cracking more difficult. The most widely used encryption algorithms are DES, 3DES, RC5, RC6, AES, and RC4. AES is the most effective of these algorithms. Symmetric encryption is employed when processing speed is required over security. Some of the most common use for symmetric encryption include: (Humadi, 2020)

- Banking and Financial organization: Encrypting the credit card information and personally Identifiable information (PII) to complete transactions.
- Data storage: encrypt data in rest.

DES (data encryption standard):

Taken into consideration, this symmetric encryption technique dates to 1976. With the use of a 56-bit encryption key, DES splits a 64-bit block into two 32-bit segments to create ciphertext from plaintext. DES is no longer in use due to security concerns. in the year 2005. The short key length of DES was a drawback since it made it simple to break using a brute-force attack. Additionally, the latest iteration of TLS (transport layer security) does not rely on DES. (Loshin, 2023)



AES (Advanced Encryption System):

Another name for it is Rijndael. NIST approved AES as an encryption standard in 2001.After the plaintext has been divided into blocks, encryption is applied. AES operates far faster than DES. AES provides many benefits, including being a quick, versatile, safe, and multiple-length key choice.AES is extensively utilized in numerous applications, including VPN, SSL/TLS protocols, mobile app encryption, wireless security, and processor security. Sensitive information is secured and protected using the AES encryption technique, which is used by numerous government organizations, including the National Security Agency (NSA).

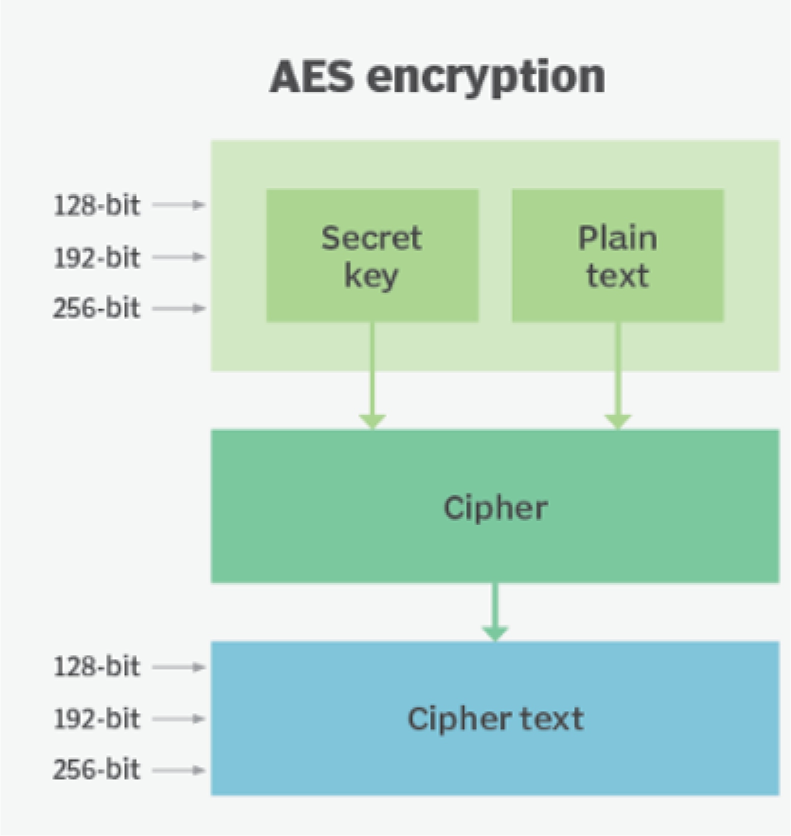


Figure from: https://www.techtarget.com/searchsecurity/definition/Data-Encryption-Standard

3DES (triple data encryption symmetric algorithm):

It is the DES algorithm in an upgraded form. It is difficult to crack since DES is applied three times for every data block. It was extensively employed in payment systems, and the financial sector incorporated TLS, SSH, IPsec, and 4OpenVPN into its cryptographic protocols. Numerous flaws in security were found. In 2019, the National Institute of Standards and Technology (NIST) prohibited of its use in draft advice for TLS 1.3, the most recent SSL/TLS protocol version that stopped using 3DES. (lake, 2023)

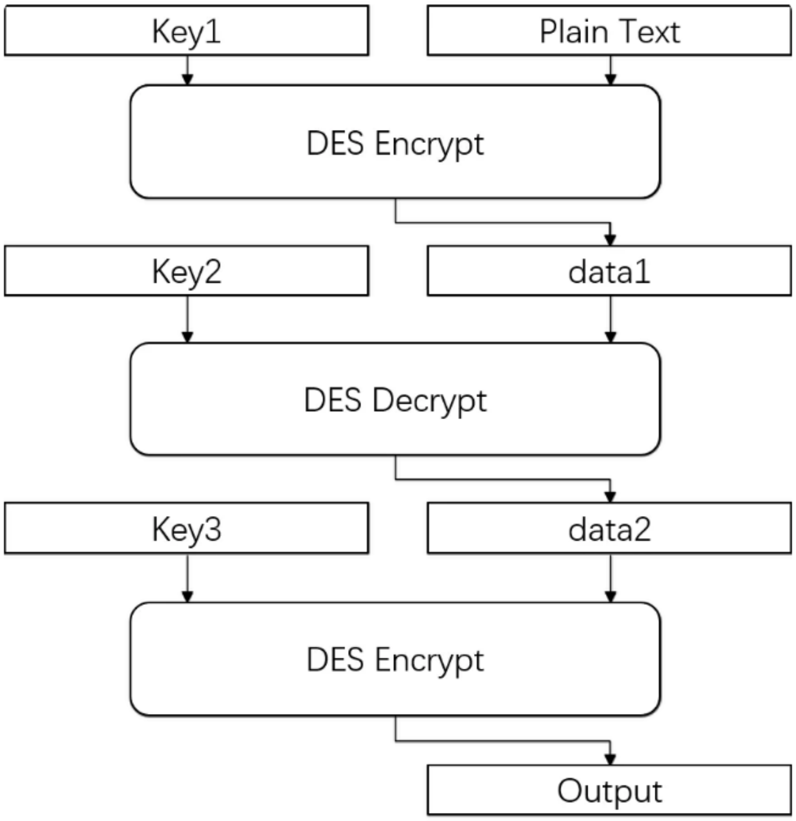


Figure from: https://xilinx.github.io/Vitis_Libraries/security/2019.2/guide_L1/internals/des.html

Challenges of Symmetric Key Cryptosystem:

- Key establishment: The secret symmetric key must be agreed upon by the sender and the recipient prior to any communication. A safe key setup system must be in place.
- Trust issue: There is an implied need that the sender and the recipient "trust" one another because they are using the same symmetric key. For instance, it could happen that the sender is unaware that the recipient has given the key to an attacker.

Asymmetric Key encryption:

Another name for it is public-key cryptography. Multiple keys are needed for both encryption and decryption. The method employs a pair of unique encryption keys that are connected to one another: a public key and a private key. Those who wish to send a message to the sender can do so by using the public key. Only the sender is aware of the second private key, which remains hidden. A private key can be used to decrypt a communication that has been encrypted with a public key. A public key can be used to decrypt a communication that has been encrypted with a private key. Since public key is accessible and can travel across the internet, security is not necessary. It is thought that asymmetric encryption is the ideal option for transmitting data. In client-server models of communication, asymmetric encryption is used. To find the server, a certificate containing the organization's profile and information is created. To ensure secure encrypted communication, the client and server send a query over the network to the other party, which responds with the certificate. Asymmetric and symmetric encryption are used by SSL/TLS. (Brush, 2023)

There is no transmission of private keys; only public keys are used in all communications. RSA, an algorithm used for authentication and encryption, and Pretty 5Good Privacy (PGP), an algorithm used for email security, are two examples of algorithms that employ this concept. When security takes precedence above speed, asymmetric encryption is employed. Common applications for asymmetric encryption include: (Rosencrance, 2023)

- Digital signature: used to confirm the identity signature.
- Blockchain: confirm the identity for the authorization transaction for cryptocurrency.
- Public key infrastructure: authorize encryption keys through the issuance of digital certificates.

RSA Asymmetric Encryption Algorithm:

Modern computers encrypt and decrypt messages using the asymmetric cryptographic method known as RSA (Rivest-Shamir-Adleman). Asymmetric cryptography, often known as public-key cryptography, uses two distinct keys for encryption and decoding. This is merely because one of the two keys can be distributed to anyone without jeopardizing the algorithm's security.

Two types of keys are used in the RSA algorithm: private and public. Since the public key is used to encrypt messages from plaintext to ciphertext, it is known to and available to everyone. However, only the matching private key will be able to decrypt messages that have been encrypted using this public key. The RSA algorithm's high degree of complexity in comparison to other cryptographic methods is what gives it its current reputation for security and dependability during the key generation process. (Asjad, 2019)

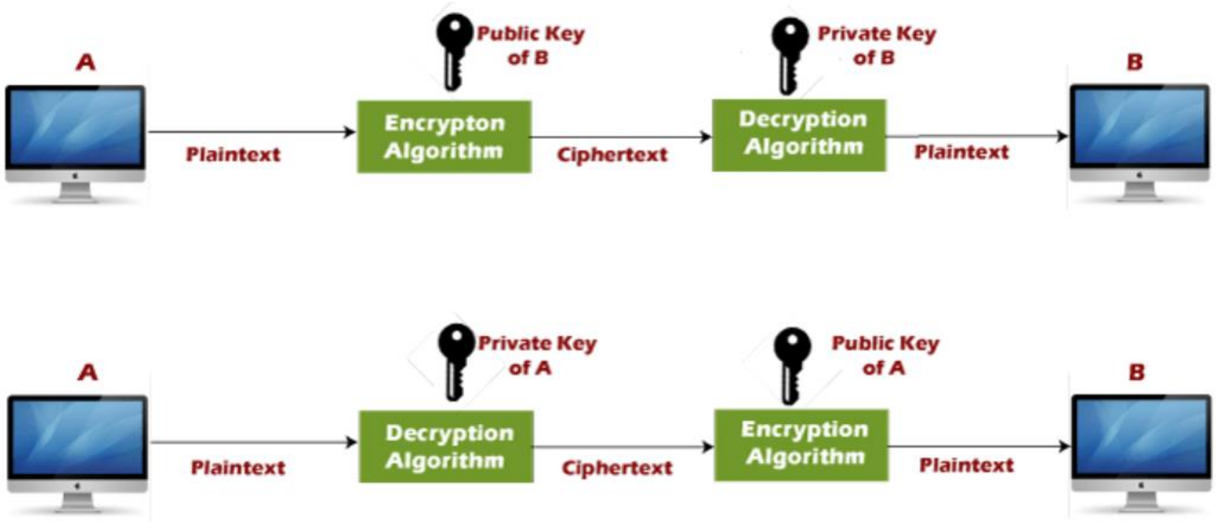


Figure from: https://www.javatpoint.com/rsa-encryption-algorithm

ECC Asymmetric Encryption Algorithm:

It is an additional kind of asymmetric encryption system. It made use of a challenging idea in mathematics, elliptic curves over finite fields. ECC has two keys: a public key that is used to validate a procedure signed with a private key, and a private key that is used to decrypt data encrypted with a public key. The best protection against existing cracking techniques is offered by ECC. With shorter key lengths, it offers RSA protection at the same level. ECC offers quicker performance and reduced strain on computer systems and networks. Applications can be encrypted using ECC encryption, which also reduces the time required for SSL/TLS handshakes when used in conjunction with an SSL/TLS certificate. ECC's drawback is that a lot of server software does not support it for SSL/TLS certificate yet. (Sullivan, 2013)

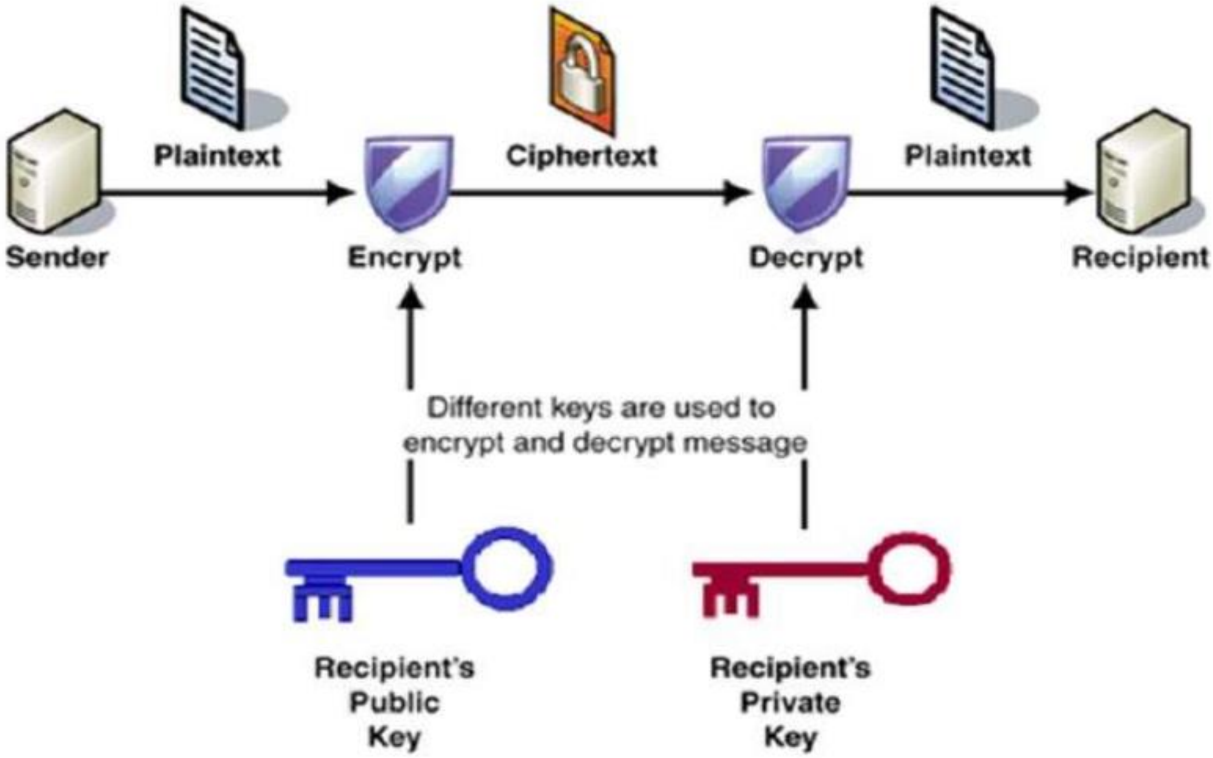


Figure from: https://www.tutorialspoint.com/cryptography/public_key_encryption.htm

The Playfair cipher

Block substitution is a feature of the symmetric polyalphabetic encryption algorithm Playfair. Although Charles Wheatstone invented it in 1954, Lord Playfair popularized its use. Another application for this cipher was as a British field cipher. Table 1 displays the 5*5 matrix that the Playfair cipher uses. (Basu, 2012)

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

Encryption:

A message is encrypted by splitting it into digraphs, or groups of two letters, which are then plotted on the key table. The matching sets of letters in the plaintext are then subjected to the subsequent protocols:

Step 1: When both alphabets lie on the identical (and pair is left with one letter only), add an "X" after the first letter then encrypt the recently developed pair and proceed with.

1. When the alphabets repose on the same row of the table, they are to be interchanged with the letters immediate right of them respectively.
2. When the alphabets repose on the same column of the table, they are to be interchanged with the letters just below them respectively.
3. When the alphabets repose not on the same row or column, exchange them with the letters on the identical row respectively but of the column of the other keeping the order of the matching set unflawed.
4. After encryption of the first digraph, pick the output and reorganize the key matrix which will be utilized to encrypt another digraph.
5. Take another diagraph and redo the steps from 1 to 5.

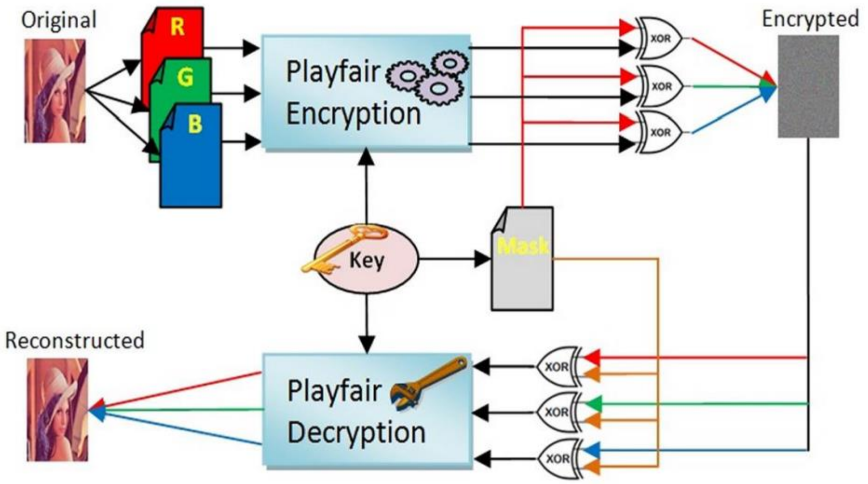


Figure from: https://ijsrcseit.com/paper/CSEIT1833311.pdf

Decryption:

A message is first divided into digraphs, or groups of two letters, and then these digraphs are mapped out on the key table to decrypt it. Then, for every matched set of alphabets in the plaintext, the ensuing procedures are used:

1. When the alphabets repose on the same row of the table, they are to be shuffled with the letters immediate left of them respectively.
2. When the alphabets repose on the same column of the table, they are to be interchanged with the letters immediately above them respectively.
3. When the alphabets do not repose on the same row or column, interchange them with the alphabets on the same row respectively but of the column of the other keeping the order of the matching set unflawed.
4. After decrypting first digraph, pick the first digraph and reorganize the key matrix. It will be used to decrypt another digraph.

Advantages:

1. It is significantly harder to break since the frequency analysis technique used to break simple substitution ciphers is difficult but still can be used on (25*25) = 625 digraphs rather than 25 monographs which is difficult.

2. Frequency analysis thus requires more cipher text to crack the encryption.

Disadvantages:

1. An interesting weakness is the fact that a digraph in the ciphertext (AB) and it's reverse (BA) will have corresponding plaintexts like UR and RU (and also ciphertext UR and RU will correspond to plaintext AB and BA, i.e., the substitution is self-inverse). That can easily be exploited with the aid of frequency analysis if the language of the plaintext is known.

2. Another disadvantage is that Playfair cipher is a symmetric cipher thus same key is used for both encryption and decryption. (Bhat, 2023)

Modified Playfair Cipher (10*9):

The 10 x 9 matrix contains almost all the printable characters. This includes lowercase and uppercase alphabets, punctuation marks, numbers, and special characters. The order of placement of different groups of characters can also be done so that the matrix formed by using the same secret keyword depends on the order of placement. This means that the ciphertext will also depend on the order of placement of different groups of characters. We can easily encrypt and decrypt any keys.

Lowercase as well as uppercase alphabets along with numbers and other printable characters can be handled. Single or multiple sentences can be encrypted and decrypted keeping the case, punctuation marks, special characters, and white space intact (white space is part of the character set which we are using). The keyword can be a word or single or multiple sentences (maximum non-duplicate character count can be 90). In case of duplicate letters in a diagram and odd number of characters we use ^ as the padding character during encryption. During decryption all instances of ^ are deleted and we get back the original plain text. The logic of substitution is same as the traditional Playfair cipher. Logics of Modified Playfair cipher are as below:

1. Table 10*9 structure

A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	a	b	c	d
e	f	g	h	i	j	k	l	m	n
o	p	q	r	s	t	u	v	w	x
y	z	0	1	2	3	4	5	6	7
8	9	~	!	@	#	$	^	&	*
?	‘	“	:	;	=	+	-	(	)
/	<	>	,	.	{	}	\	_	

2. Spacing characters and symbols
3. Modified from 25 letters to 90 letters.
4. Using ^ as fill up character for duplicate letters.

Why modification was necessary:

1. Limited Character Set in Traditional Playfair Cipher:
   - In the traditional Playfair cipher, the plaintext is restricted to 25 uppercase letters. One letter must be omitted, and lowercase letters, white space, numbers, and other printable characters cannot be handled.
   - This limitation prevents the encryption and decryption of complete sentences, or a wider range of characters commonly found in text.
2. Monoalphabetic vs. Polyalphabetic Cipher:
   - In a monoalphabetic cipher, the attacker only needs to search in 26 letters. However, Playfair being a polyalphabetic cipher requires the attacker to search in 26 x 26 = 676 diagram, making frequency analysis more complex but not immune to modern computational techniques.
3. Handling Duplicate Letters and Padding:
   - The modified cipher addresses the issue of duplicate letters in a digram and odd numbers of characters by using '^' as a padding character during encryption. During decryption, instances of '^' are deleted to obtain the original plaintext.
4. Increased Key Space:
   - The modified cipher claims to have a larger key domain (90!) compared to the traditional Playfair cipher, making brute-force attacks significantly more difficult.
5. Cryptanalysis:
   - The paper discusses various types of cryptanalytic attacks, such as brute force, ciphertext-only, and chosen plaintext/ciphertext attacks. It suggests that the modified Playfair cipher is stronger than the original one, especially in terms of the increased key space.

New methodology implied:

1. Key Generation:
   - Choose a secret keyword or key phrase (e.g., "Hello lets meet tonight at 5:00 pm").
   - Define the order of character groups (e.g., lowercase, uppercase, numbers, special characters).

2. Matrix formation:
   - Create a 10 x 9 matrix using the chosen character groups and the secret keyword.
   - Handle duplicate characters appropriately.
   - Sequence of character groups may affect the matrix, enhancing security.

3. Encryption:
   - Break the plaintext into diagram.
   - Handle duplicate letters and odd characters with padding ('^').
   - For each diagram:
     - Apply the Playfair substitution rules using the 10 x 9 matrix.
     - Rules:
     - If letters are in the same row, replace with the letters to their right (circular).
     - If in the same column, replace with the letters below (circular).
     - If forming a rectangle, replace with the letters in the same row but the column of the other letter.
     - Output the encrypted ciphertext.
4. Decryption:
   - Break the ciphertext into diagram.
   - For each diagram: Apply the reverse of the Playfair substitution rules using the same matrix.
   - Remove any padding characters ('^').
   - Output the decrypted plaintext.
5. Cryptanalysis:
   - Brute force attack: The key domain is 90! (factorial 90), making brute force difficult.
   - Ciphertext Only attack: Frequency analysis is complex with 90 x 90 = 8100 diagram

- Chosen Plaintext/Ciphertext Attack: Knowledge of both plaintext and ciphertext is required for key recovery.

Algorithm:

Encryption algorithm:

Step 1: Use the secret keyword to generate a key for the matrix and define the order of character groups.

Step 2: Create a 10*9 matrix using the character groups and the generated key. Handle duplicate characters appropriately and sequence of characters groups may affect the matrix, enhancing security.

Step 3: Break the plaintext inti digrams and handle duplicate letters an odd character with padding (^).

Step 4: Locate the positions of the two letters in the matrix. Apply Playfair substitution rules:

- If in the same column, replace with the letters below (circular).
- If letters are in the same row, replace with the letters to their right (circular).
- If forming a rectangle, replace with the letters in the same row but the column of the other letter.
- Output: Encrypted cipher text.

Step 4: Return the encrypted cipher text.

Decryption algorithm:

Step 1: Use the secret keyword to generate a key for the matrix and define the order of character groups.

Step 2: Create a 10*9 matrix using the character groups and the generated key. Handle duplicate characters appropriately and sequence of character groups may affect the matrix, enhancing security.

Step 3: locate the positions of the two letters in the matrix. Apply the reverse Playfair substitution rules:

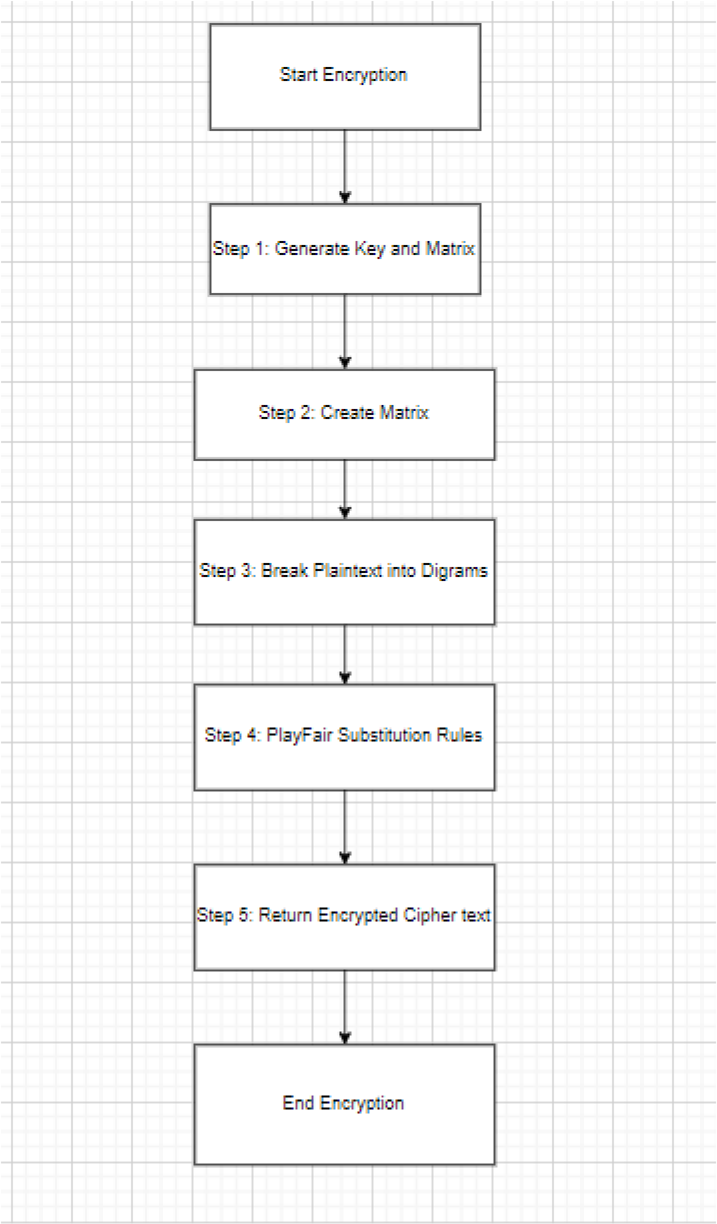
- If letters are in the same row, replace with the letters to their left (circular).
- If in the same column, replace with the letters above (circular).
- If forming a rectangle, replace with the letters in the same row but the column of the other letter.

Step 4: Remove any padding characters (^).

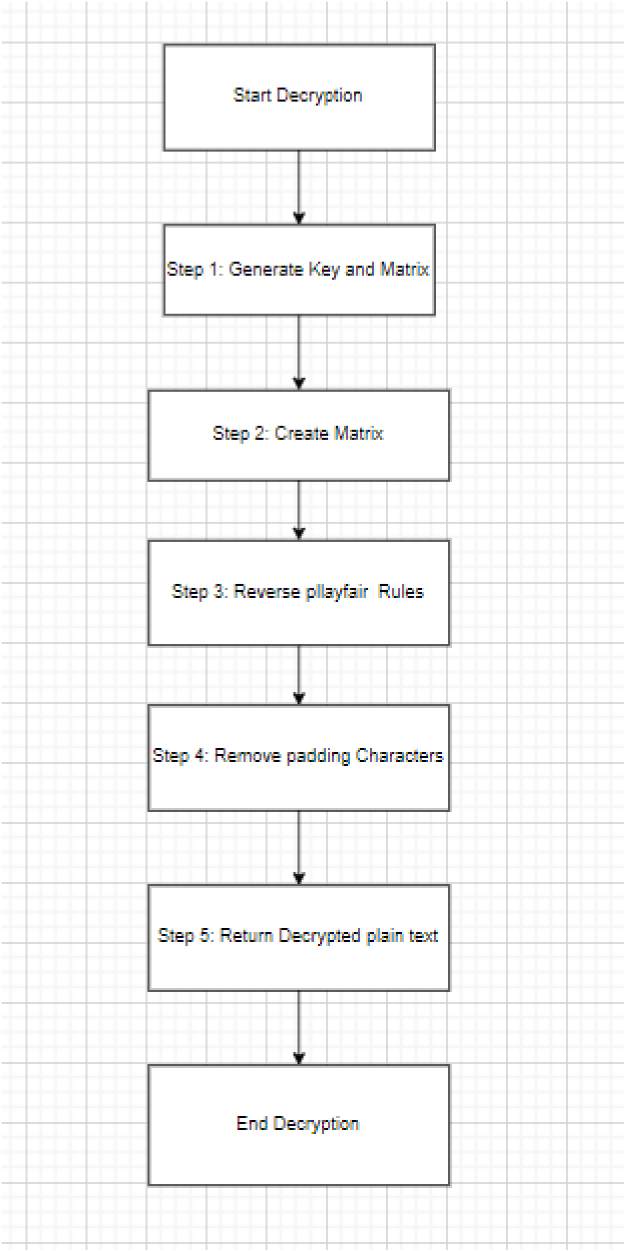
Step 5: Return the decrypted plaintext.

Flow chart:

Encryption:


Start Encryption
Step 1: Generate Key and Matrix
Step 2: Create Matrix
Step 3: Break Plaintext into Digrams
Step 4: PlayFair Substitution Rules
Step 5: Return Encrypted Cipher text
End Encryption

Decryption:


Start Decryption
Step 1: Generate Key and Matrix
Step 2: Create Matrix
Step 3: Reverse pllayfair Rules
Step 4: Remove padding Characters
Step 5: Return Decrypted plain text
End Decryption

STRENGTH, WEAKNESS, OPPRTUNITY, AND THREAT ANALYSIS

Strengths:

1. The modified Playfair cipher accommodates almost all printable characters, including lowercase and uppercase alphabets, punctuation marks, numbers, and special characters. This significantly increases the complexity of the cipher.
2. The claim of having a larger key domain (90!) compared to the traditional Playfair cipher makes brute-force attacks significantly more challenging. The increased key space adds to the overall strength of the encryption.

3. The dependence of the ciphertext on the order of placement of different character groups adds an extra layer of security. Even if an attacker knows the keyword, the specific arrangement of character groups affects the matrix, making cryptanalysis more challenging.

Weakness:

1. While the modified Playfair cipher is polyalphabetic, making frequency analysis more challenging than in monoalphabetic ciphers, it may still be susceptible to more advanced frequency-based attacks, especially with larger datasets.
2. In situations where the attacker has access to both the plaintext and corresponding ciphertext, they might have an easier time deducing patterns in the encryption process, potentially leading to key recovery.
3. If an attacker knows that the '^' character is used as padding for duplicate letters, they might attempt to exploit this knowledge in a known-plaintext attack.

Opportunity:

1. Researchers and cryptographers have an opportunity to experiment with various techniques for key generation within the context of the modified Playfair cipher. Exploring alternative methods for generating the key could lead to enhancements in security.
2. The modified Playfair cipher can handle a wide range of data types, including lowercase and uppercase alphabets, punctuation marks, numbers, and special characters. This versatility allows for the encryption and decryption of diverse content while preserving the structure of the original message.

Threat:

1. Brute force attacks involve trying all possible keys until the correct one is found. The large key space (90!) theoretically makes brute force difficult, but with increasing computational power, it remains a potential threat.
2. Even though the modified Playfair cipher is polyalphabetic, sophisticated frequency analysis techniques may be applied to detect patterns and exploit redundancies.

Test:1

Key: Hello lets meet tonight at 5:00 pm

H	e	l	o		t	s	m	n	i
g	h	a	5	:	0	p	A	B	C
D	E	F	G	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X
Y	Z	a	b	c	d	f	j	k	p
q	r	u	v	w	x	y	z	1	2
3	4	6	7	8	9	/	!	@	#
$	%	^	&	*	(	)	-	+	=
<	>	{	}	?	~	;	‘	,	.

Encryption using Modified cipher (10*9):

Let us take the plaintext as Hey bro what’s up! Breaking up the plaintext into diagrams we get the following diagrams and hence the ciphertext.

He We can see they are in same rows. Using rule 2 we get el.

Y(space) They are neither in same row nor column. Using rule 4 we get c H

b r They are neither in same row nor column. Using rule 4 we get Z v

o(space) They are in same row. Using rule 2 we get (space)t

w h They are neither in same row nor column. Using rule 4 we get r:

t’ They are neither in same row nor column. Using rule 4 we get m~

s(space) They are in same row. Using rule 2 we get mt

up They are neither in same row nor column. Using rule 4 we get ya

! ^ They are neither in same row nor column. Using rule 4 we get 6-

Decryption using Modified cipher (10*9):

In the case of decryption rules 2 and 3 must be reversed. Breaking up the cipher text into digrams we get the following diagram and hence the plaintext.

e l We can see they are in the same rows. Using rule 2 we get He

c H They are neither in same row nor column. Using rule 4 we get Y(space)

Z v They are neither in same row nor column. Using rule 4 we get b r
(space)t They are in same row. Using rule 2 we get o(space)
r: They are neither in same row nor column. Using rule 4 we get w h
m~ They are neither in same row nor column. Using rule 4 we get t'
mt They are in same row. Using rule 2 we get s(space)
ya They are neither in same row nor column. Using rule 4 we get up
6- They are neither in same row nor column. Using rule 4 we get !^

Test2:
Plain text: I$LinGT0N
Encryption:
I$ we get D*.
Li we get Nm.
Gt we get jo.
T0 we get dj
N^ we get F=

Decryption:
D* we get I$
Nm we get Li
jo we get Gt
dj we get T0
F= we get N (because in decryption part we remove padding i.e ^)

Test 3:
Plain text: Nepal
Encryption:
Ne we get Ei
Pa we get Yb
l^ we get a{

Decryption:
Ei we get Ne
Yb we get pa
a{ we get l

Test 4:
Plain text: Bibidh
Encryption:
Bi we get Cn
bi we get po
dh we get Z0

Decryption:
Cn we get Bi
po we get bi
Z0 we get dh

Test 5:
Plain text: Good
Encryption:
Go we get R5
od we get tb

Decryption:
R5 we get Go
tb we get od