



Cyber Security

Assignment 1

Course: BSc Computer Science

Module: Cyber Security

Module Leader:

Module Tutor:

Student: Nunzio Emanuele Sgroi

Student ID:

Academic Year
2023/2024

Table of Contents

1. Introduction to Encryption and the Playfair Cipher	2
2. The Playfair Cipher Explained	2
2.1. Key Matrix Creation	2
2.2. Encryption Process.....	3
2.3. Decryption Process	4
3. Proposed Changes to the Playfair Cipher	5
3.1. Matrix Design for the Proposed Model	5
3.2. The Encryption Process in the Revised Model.....	6
3.2.1. Example of Encryption process with the Proposed Model.....	7
3.3. The Decryption Process in the Revised Model	8
3.3.1. Example of Decryption process with the Proposed Model	8
4. Discussion and Conclusion	10
5. References	10

Table of Figures

Figure 1 - Text Segmentation into Diagraph	4
Figure 2 - Example of Text Shifting for the Step 1 Encryption of the Proposed Model.....	6
Figure 3 - Example of Second Matrix Lookup for the Step 3 Encryption of the Proposed Model.....	7

List of Tables

Table 1 - 5x5 Matrix: Keyword Integration	3
Table 2 - Complete 5x5 Matrix with Predeterminate Keyword.....	3
Table 3 - Playfair Cipher Encryption Process	4
Table 4 - Playfair Cipher Decryption Process	5
Table 5 - 10x10 Matrix of the Proposed Model with Keyword and 3-digit code Predeterminate	6
Table 6 - Step 1 of the Encryption Process of the Proposed Model	7
Table 7 - Step 2 of the Encryption Process of the Proposed Model	8
Table 8 - Step 3 of the Encryption Process of the Proposed Model	8
Table 9 - Step 1 of the Decryption Process of the Proposed Model.....	9
Table 10 - Step 2 of the Decryption Process of the Proposed Model.....	9
Table 11 - Step 3 of the Decryption Process of the Proposed Model.....	9

Student: Nunzio Emanuele Sgroi

Student ID:

1. Introduction to Encryption and the Playfair Cipher

Encryption has been a cornerstone of secure communication since ancient times, beginning with the non-standard hieroglyphs used by the Egyptians around 1900 BC. This practice, evolving significantly over the centuries, has been foundational to modern cybersecurity. Cryptography, originating from the Greek words "kryptos" for "hidden" and "graphy" for "writing," reflects the core of secret communication through the ages (A. Mardon et al., 2021).

Among historical encryption methods, the Caesar Cipher emerged as an early system, shifting alphabet letters to encode messages—a method attributed to Julius Caesar. Yet, it was the Playfair cipher, invented by Charles Wheatstone and popularized by Baron Lyon Playfair in the mid-19th century, that marked a significant advancement in encryption techniques. This cipher, encrypting letters in pairs, effectively countered frequency analysis, a common cryptanalytic attack, enhancing the security of military and diplomatic messages during pivotal historical moments such as the Boer Wars and World War I (T. Huber, 2010).

The transition from simple ancient ciphers to the more complex Playfair cipher underscores the continuous evolution of encryption strategies to meet the demands of secure communication. The Playfair cipher's innovative approach to letter encryption represents a crucial development in the history of cryptography, setting the stage for the sophisticated algorithms that safeguard digital communications today.

2. The Playfair Cipher Explained

Diving further into the intricacies of the Playfair Cipher, by focusing on pairs of letters, or digraphs, this encryption technique presented a more complex challenge for potential codebreakers, sidestepping the vulnerabilities to frequency analysis that single-letter encryption methods faced, as mentioned earlier. This section aims to elucidate the process of setting up the cipher through its key matrix and explicates the procedures for both encryption and decryption, shedding light on why this method has been historically significant.

2.1. Key Matrix Creation

At the heart of the Playfair cipher lies the key matrix, a 5x5 grid filled with letters of the alphabet. This matrix serves as the cipher's foundation, determining the substitution for each letter pair during the encryption and decryption processes. The matrix is constructed using a keyword or phrase, ensuring that each letter in the alphabet appears only once. To accommodate all 26 letters of the English alphabet into a 25-square grid, the letters "I" and "J" are typically merged (A. Kumar et al., 2013).

To facilitate comprehension, the following paragraphs provide a comprehensive explanation of the matrix construction process using my middle name "Emanuele" as the keyword.

1. **Keyword Integration:** The initial step involves incorporating the unique letters of the keyword "Emanuele" into the grid. Due to the presence of duplicate letters, specifically the letter "E" appearing multiple times, only the first occurrence is considered. Consequently, the distinct characters that form the basis of the grid are "EMANUL".

E	M	A	N	U
L				

Table 1 - 5x5 Matrix: Keyword Integration

2. **Completing the Grid:** Following the keyword placement, the remaining cells of the grid are filled with the rest of the alphabet in order, omitting any letters already included through the keyword, and combining "I" and "J" as mentioned above.

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

Table 2 - Complete 5x5 Matrix with Predeterminate Keyword

The construction of the key matrix in the Playfair cipher represents a fundamental step in the encryption and decryption process. By embedding a keyword into a 5x5 grid and populating the remaining spaces with the rest of the alphabet, this cipher ingeniously masks the plaintext, rendering it unintelligible to unauthorized parties. The choice of keyword is critical, as it personalizes the cipher to the user's specifications, thereby enhancing security (geekforgeeks.org, 2023).

2.2. Encryption Process

The encryption process in the Playfair Cipher transforms plaintext into ciphertext through a mechanism that leverages a key matrix. This key matrix, previously established with the keyword "Emanuele" as an example, serves as the foundation for encrypting pairs of letters, known as digraphs. The process ensures an even number of characters for encryption by potentially appending an "X" to the plaintext to form complete digraphs. These digraphs then undergo encryption according to their positional relations within the key matrix, adhering to specific rules designed to obfuscate the original message effectively (geekforgeeks.org, 2023).

The rules for encrypting digraphs are as follows:

1. **Same Row Rule:** If two letters appear in the same row of the key square, they are replaced by the letters to their right, wrapping around to the beginning of the row if needed.
2. **Same Column Rule:** If two letters appear in the same column of the key square, they are replaced by the letters below them, wrapping around to the top of the column if needed.
3. **Rectangle Rule:** If two letters are not in the same row or column, imagine a rectangle drawn around them in the key square. The letters are then replaced by the letters at the opposite corners of the rectangle.

The following example aims to encrypt the message "HELLO WORLD", which after adjusting it for the Playfair Cipher's requirements (removing spaces and adding "X" to ensure an even number of characters) results in "HELXLOWORLDX". The message is then segmented into digraphs: HE LX LO WO RL DX.

Student: Nunzio Emanuele Sgroi

Student ID:

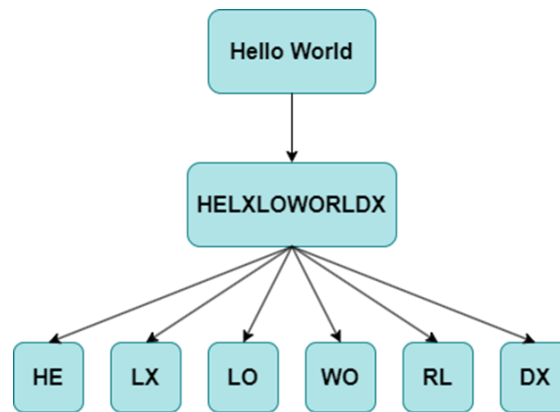


Figure 1 - Text Segmentation into Digraph

At this point the algorithm would encrypt each digraph following the rules highlighted in this section:

Digraphs	Algorithm Explanation	Encrypted Digraph
HE	Forms a rectangle: H to G, E to M	GM
LX	Forms a rectangle: L to C, X to V	CV
LO	Forms a rectangle: L to F, O to G	FG
WO	Forms a rectangle: W to Z, O to H	ZH
RL	Forms a rectangle: R to P, L to C	PC
DX	Forms a rectangle: D to C, X to Y	CY

Table 3 - Playfair Cipher Encryption Process

After combining the encrypted digraph, the final encrypted message is: "GMCVFGZHPCCY".

2.3. Decryption Process

The decryption process in the Playfair Cipher reverses the encryption mechanism to transform ciphertext back into plaintext, utilizing the same key matrix established for encryption. For our discussion, the key matrix built with the keyword "Emanuele" will continue to serve as the reference. This process requires the ciphertext to be divided into digraphs, identical to the encryption stage, and then decrypted according to their positions within the key matrix. The reversal of encryption rules applied to these digraphs reveals the original message, demonstrating the cipher's ability to securely encrypt and decrypt messages while maintaining their integrity (geekforgeeks.org, 2023).

The rules for decrypting digraphs mirror those of encryption:

1. **Same Row Rule:** If both letters of a digraph reside in the same row, each letter is replaced by the letter immediately to its left, wrapping around to the end of the row if necessary.
2. **Same Column Rule:** If both letters are in the same column, each letter is substituted with the letter directly above it, with wrapping to the bottom of the column when reaching the top.
3. **Rectangle Rule:** If the letters of the digraph do not share a row or column, they form two corners of a rectangle within the matrix. Each letter is decrypted by replacing it with the letter at the opposite corner of the rectangle on the same row.

Student: Nunzio Emanuele Sgroi

Student ID:

For the decryption algorithm, the message is also segmented into digraphs: GMCVFGZHPCCY → GM CV FG ZH PC CY. Following the decryption rules, each digraph is decrypted as shown:

Digraphs	Algorithm Explanation	Decrypted Digraph
GM	Forms a rectangle: G to H, M to E	HE
CV	Forms a rectangle: C to L, V to X	LX
FG	Forms a rectangle: F to L, G to O	LO
ZH	Forms a rectangle: Z to W, H to O	WO
PC	Forms a rectangle: P to R, C to L	RL
CY	Forms a rectangle: C to D, Y to X	DX

Table 4 - Playfair Cipher Decryption Process

After reassembling the decrypted digraphs, the message obtained is "HELXLOWORLDX". Recognizing "X" as a potential filler used during encryption and knowing the original formatting requirements of the Playfair Cipher, careful interpretation is applied to remove unnecessary Xs and reintroduce spaces where appropriate. This nuanced step restores the message to its original form, "HELLO WORLD", demonstrating the decryption process's effectiveness while acknowledging the manual adjustments needed for complete accuracy.

3. Proposed Changes to the Playfair Cipher

The traditional Playfair Cipher, while a significant innovation at the time of its conception, is primarily tailored for the encryption of alphabetic text. This inherent limitation significantly undermines its utility in the contemporary digital landscape, where the composition of passwords and messages frequently encompasses a comprehensive mix of characters, including but not limited to numbers, symbols, and spaces. In recognition of these constraints, the proposed revision aims to modernize the Playfair Cipher to accommodate a broader spectrum of characters. The introduction of a dual-matrix encryption system, along with reinforced rules for both encryption and decryption, substantially enhances the security measures of the cipher. This adaptation not only extends its applicability to modern requirements of digital communication but also ensures a more robust defence against both common and advanced cryptanalysis techniques. By incorporating a dual-matrix system, the character set is diversified, and an additional layer of encryption complexity is introduced. This modification significantly improves the cipher's resilience against potential attacks, thereby elevating its efficacy and relevance for securing digital communications in the current era.

3.1. Matrix Design for the Proposed Model

Moving beyond the traditional 5x5 matrix of the original Playfair Cipher, this updated approach introduces a foundational 10x10 matrix, significantly enlarging the encryption landscape to include two such matrices for improved security. This expanded format now supports a full array of characters, covering both uppercase and lowercase letters, digits, symbols, and even space, enhancing the cipher's versatility.

Similar to the classic model, a case-sensitive keyword initializes the first matrix, ensuring no letter is repeated within the grid (considering the distinction between uppercase and lowercase). Following the letters are the numbers, which require a 3-digit code that populate the first three slots. Similar

Student: Nunzio Emanuele Sgroi

Student ID:

to letters, numbers within the keycode cannot be repeated. Symbols and a space fill the remaining entries, sequenced by a predetermined order.

In contrast, the second matrix reverses the order of the first, yet both matrices adhere to the same keyword and keycode protocol.

The example below demonstrates a single 10x10 matrix constructed for this new approach, incorporating the keyword "EmAnUeLe" and the 3-digit code "273" (note that a second, reversed matrix would be used in the actual encryption process).

E	m	A	n	U	e	L	B	C	D
F	G	H	I	J	K	M	N	O	P
Q	R	S	T	V	W	X	Y	Z	a
b	c	d	f	g	h	i	j	k	l
o	p	q	r	s	t	u	v	w	x
y	z	2	7	3	0	1	4	5	6
8	9	`	-		!	“	£	\$	€
%	^	&	*	()	-	_	=	+
[]	{	}	;	:	'	@	#	~
\		,	<	.	>	/	?	¥	

Table 5 - 10x10 Matrix of the Proposed Model with Keyword and 3-digit code Predetermine

3.2. The Encryption Process in the Revised Model

As part of the two-matrix system, the proposed Playfair Cipher variation introduces distinct encryption rules compared to the classic version. This aims to enhance the algorithm's security.

Similar to the classic approach, the message is first divided into digraphs. However, unlike the classic method, even-length messages are not required. The message length itself plays a crucial role in the encryption process. If the message has an odd number of characters, the last digraph will consist of a single character.

The encryption process follows three steps:

1. **Text Length Shift:** All characters are shifted forward within the 10x10 matrix by an amount equal to the text length. This shift wraps around to the beginning of the matrix if necessary.

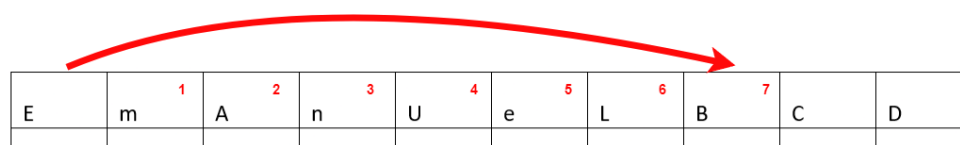


Figure 2 - Example of Text Shifting for the Step 1 Encryption of the Proposed Model

2. **Classic Playfair Cipher Rules (with Exception):** After the shift, the classic Playfair Cipher rules (same row, same column, rectangle rule) are applied to each digraph. If the message length is odd, the final character (single-character digraph) undergoes another message length shift.
3. **Second Matrix Lookup:** Finally, the encrypted characters are located within the second (reversed) matrix (see example below). The final encrypted character is the one found in the second matrix.

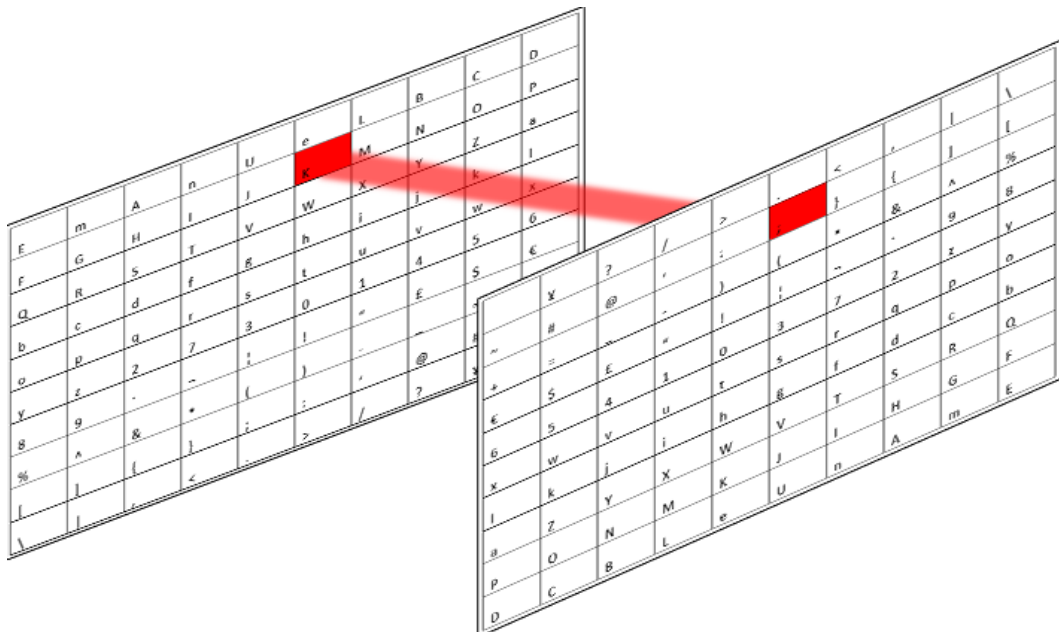


Figure 3 - Example of Second Matrix Lookup for the Step 3 Encryption of the Proposed Model

3.2.1. Example of Encryption process with the Proposed Model

This example demonstrates the encryption process using the message "Uwl 24@" and the previously established matrices constructed with the keyword "EmAnUeLe" and 3-digit code "273". Segmenting the message into digraphs results in "Uw", "l[space]", "24", and "@" (note that "@" forms a single-character digraph, indicating an odd number of characters in the message). The encryption process will also consider the text length (7 in this case).

Starting with the first step, all characters are shifted forward by 7 slots within the first 10x10 matrix.

Digraphs	Algorithm Explanation	Encrypted Digraphs
Uw	Shift 7 slots forward: U to G, w to 0	G0
l[space]	Shift 7 slots forward: l to u, [space] to L	uL
24	Shift 7 slots forward: 2 to 6, 4 to	6
@	Shift 7 slots forward: @ to .	.
Encrypted text of step 1: G0uL6 .		

Table 6 - Step 1 of the Encryption Process of the Proposed Model

The initial step yields the first layer of encryption, producing "G0uL6|.". Subsequently, the classic Playfair Cipher encryption rules are applied to this outcome. Given that the final digraph consists of

a single character, this character undergoes an additional shift forward by 7, in line with the first step's logic.

Digraphs	Algorithm Explanation	Encrypted Digraphs
G0	Forms a rectangle: G to K, 0 to z	Kz
uL	Same column: u to i, L to /	i/
6!	Forms a rectangle: 6 to 3, ! to €	3€
.	Shift 7 slots forward: . to m	m
Encrypted text of step 2: Kzi/3€m		

Table 7 - Step 2 of the Encryption Process of the Proposed Model

The second layer of encryption yields "**Kzi/3€m**". The final step involves replacing each character with its corresponding character from the reversed matrix, as previously explained.

Digraphs	Algorithm Explanation	Encrypted Digraphs
Kz	Swap with corresponding: K to ;, z to w	;w
i/	Swap with corresponding: i to -, / to n	-n
3€	Swap with corresponding: 3 to t, € to b	tb
m	Swap with corresponding: m to ¥	¥
Encrypted text of step 3: ;w-ntb¥		

Table 8 - Step 3 of the Encryption Process of the Proposed Model

The final encrypted message is "**;w-ntb¥**". This process transforms **Uwl 24@** into **;w-ntb¥**, utilizing dual matrices and three layers of encryption, thereby providing a significantly higher level of security than the classic Playfair Cipher.

3.3. The Decryption Process in the Revised Model

The decryption process in the revised model mirrors the encryption process, utilizing the same keyword and 3-digit code to generate the dual matrix. However, the steps are performed in reverse order:

1. **First Matrix lookup:** Locate the encrypted characters within the first matrix. Unlike the encryption process, swap them with their corresponding characters from the first matrix.
2. **Classic Playfair Cipher Rules (with Exception):** Classic decryption rules are applied at the second step, with the exception that if the last digraph contains only one character, then this will be shifted backward a number of times equivalent to the length of the text that needs to be decrypted.
3. **Message Length Shift:** All characters are shifted backward within the 10x10 matrix by an amount equal to the text length. This shift wraps around to the beginning of the matrix if necessary.

3.3.1. Example of Decryption process with the Proposed Model

This example demonstrates how the ciphertext "**;w-ntb¥**" undergoes decryption using the established rules for the proposed Playfair Cipher expansion and the previously created dual matrix

Student: Nunzio Emanuele Sgroi

Student ID:

system. Mirroring the encryption process, the text is first segmented into digraphs (pairs of characters). The length of the text is then determined, which is 7 characters in this case.

In the initial step, the process involves replacing each encrypted character with its corresponding character found within the first matrix.

Digraphs	Algorithm Explanation	Decrypted Digraphs
;w	Swap with corresponding: ; to K, w to z	Kz
-n	Swap with corresponding: - to i, n to /	i/
tb	Swap with corresponding: t to 3, b to €	3€
¥	Swap with corresponding: ¥ to m	m
Decrypted text of step 1: Kzi/3€m		

Table 9 - Step 1 of the Decryption Process of the Proposed Model

The second step applies classic decryption rules, except for the last character, which is shifted backward by 7 slots.

Digraphs	Algorithm Explanation	Decrypted Digraphs
Kz	Forms a rectangle: K to G, z to 0	G0
i/	Same column: i to u, / to L	uL
3€	Forms a rectangle: 3 to 6, € to †	6†
m	Shift 7 slots backward: m to .	.
Decrypted text of step 1: G0uL6†.		

Table 10 - Step 2 of the Decryption Process of the Proposed Model

Finally, all characters are shifted backward 7 slots.

Digraphs	Algorithm Explanation	Decrypted Digraphs
G0	Shift 7 slots backward: G to U, 0 to w	Uw
uL	Shift 7 slots backward: u to l, L to [space]	l[space]
6†	Shift 7 slots backward: 6 to 2, † to 4	24
.	Shift 7 slots backward: . to @	@
Decrypted text of step 1: Uwl 24@		

Table 11 - Step 3 of the Decryption Process of the Proposed Model

The decryption algorithm successfully returned the text "**Uwl 24@**" which matches the original text used for the encryption example. This demonstrates compatibility between the decryption and encryption algorithms.

4. Discussion and Conclusion

The advancement of the Playfair Cipher with a dual-matrix system marks a substantial improvement in encryption technology. Expanding the character set to include numbers, symbols, and spaces, the model overcomes a key limitation of the traditional cipher, enhancing its relevance for digital communication.

However, this model does present weaknesses worth noting. The added complexity of encryption and decryption processes could affect computational efficiency, impacting scenarios requiring quick data processing. Furthermore, the introduction of a keyword and a 3-digit code complicates key management, potentially increasing security risks. Additionally, the expanded character set and dual-matrix system might introduce vulnerabilities exploitable by cryptanalysts, particularly if predictable patterns emerge.

In conclusion, the enhancements to the Playfair Cipher greatly bolster its security and applicability for contemporary encryption needs, yet they also introduce challenges. Balancing security enhancements with operational efficiency and secure key management remains critical. Addressing these weaknesses is essential for the cipher's reliability and effectiveness in securing digital communications amidst evolving digital challenges.

5. References

- A. Kumar et al. (2013). Enhanced Block Playfair Cipher. *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness* (pp. 689-695). Springer, Berlin, Heidelberg. doi:https://doi.org/10.1007/978-3-642-37949-9_60
- A. Mardon et al. (2021). Cryptography Online. (A. Yermolenko, Ed.) Retrieved February 26, 2024, from https://d1wqtxts1xzle7.cloudfront.net/70204417/Cryptography_Online-libre.pdf?1632532209=&response-content-disposition=inline%3B+filename%3DCryptography_Online.pdf&Expires=1710179811&Signature=CcyD9K-9-06l2RfW-yM-lsgpTHQj-Y0x3E3ERWsv3Pq2IGrzt6TRUXLx9jHviZr
- geekforgeeks.org. (2023). *Playfair Cipher with Examples*. Retrieved March 10, 2024, from [geekforgeeks.org: https://www.geeksforgeeks.org/playfair-cipher-with-examples/](https://www.geeksforgeeks.org/playfair-cipher-with-examples/)
- T. Huber. (2010). Wheatstone-Playfair Cipher. 1-6. Retrieved from <https://derekbruff.org/blogs/fywscrypto/files/2010/11/Huber-Essay-2.pdf>