Revista de la Facultad de Contaduría y Ciencias Administrativas

Universidad Michoacana de San Nicolás de Hidalgo
Cuna de héroes, crisol de pensadores

LA CRIPTOGRAFÍA CLÁSICA EN LA PRIVACIDAD Y PROTECCIÓN DE DATOS

CLASSIC CRYPTOGRAPHY APPLIED IN DATA SECURITY

Pedro Chávez Lugo (✉) [1].

Universidad Michoacana de San Nicolás de Hidalgo [1]

México

Recibido el 5 de Octubre de 2018; Aceptado el de 10 Diciembre de 2018; Disponible en Internet el 20 de Diciembre de 2018

E-mail de Correspondencia: pchavezl@umich.mx

Vol. 3, Nº 6 Pág. 89-96. ISSN: 2448-6051

Av. Gral. Francisco J. Múgica S/N
Edificio AII C.P. 58030
Ciudad Universitaria
Morelia, Michoacán, México.
Tel. y Fax (443) 3-16-74-11
Email: rfcca@umich.mx
Web: http://rfcca.umich.mx.

Resumen

La sociedad debido al uso constante de las TIC's en sus actividades rutinarias demanda el cumplimiento de la privacidad, confidencialidad e integridad de los datos personales o laborales. La criptografía es la mejor alternativa para satisfacer estas necesidades mediante el uso de software criptográfico comercial o de código abierto. Una de las desventajas del software criptográfico comercial o de código abierto es el manejo de firmas en el contenido de los datos cifrados, lo cual pone en evidencia el o los métodos de cifrado utilizados para proteger la información. Una opción para el ocultamiento de tales firmas es el uso de los métodos criptográficos clásicos sobre los métodos utilizados por el software comercial o de código abierto. De esta forma los patrones de firma en los datos cifrados serán ocultados mediante los métodos clásicos de transposición por columnas, reversa y Vigenère. Este trabajo propone una alternativa criptográfica que combine los métodos criptográficos clásicos a elección del usuario, y para esto generara un archivo con la especificación del orden y especificación de los métodos utilizados. La meta es ofrecerle a sociedad una alternativa adicional para proteger sus datos sensibles mediante el uso de los métodos criptográficos clásicos.

Palabras Clave: Criptografía, Clásica, Reversa, Transposición, Vigenère.

Abstract

Nowadays, the society employs a constant use of TIC's in personal or work routines, these activities requires compliance data privacy, confidentiality and integrity. Cryptography is the best alternative to satisfy these needs through the use of commercial or open source encryption software. One of the disadvantages of commercial or open source encryption software shows signatures in the content of the encrypted data used in data protection. One option for hide signatures are the classical cryptography methods applied over the methods used by commercial or open source encryption software. This work proposes an alternative for combines classic cryptography methods – columnar transposition, reverse and Vigenère selected by an user. The encryption key corresponds a file within the order of the classic cryptography methods used. The goal is an additional alternative for the society to protect their sensitive data through the use of classic cryptography methods.

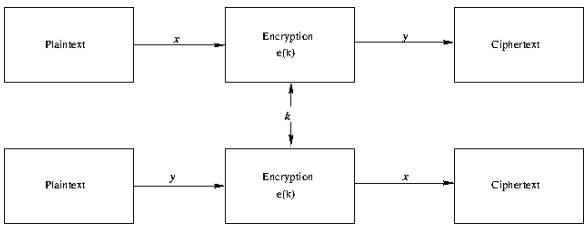
Keywords: Cryptography, Classic, Reverse, Transposition, Vigenère.

INTRODUCCION

La criptografía es una antigua herramienta utilizada por el hombre para ocultar información sensible. Con anterioridad la criptografía era utilizada solo por militares y diplomáticos, pero actualmente es utilizada en todos los ámbitos del ser humano, en el comercio, la comunicación, los datos personales, etc. Una definición actual de la criptografía la define como el estudio de las técnicas matemáticas utilizadas en el ocultamiento de la información (Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996)), (Swenson, C. (2008)). La criptografía ha evolucionado desde sus principios clásicos de cifrado hasta las técnicas matemáticas relacionadas con la criptografía de curvas elípticas.

Dentro de la criptografía se presentan los procedimientos simétricos y asimétricos. Para el caso de los procedimientos simétricos en el proceso de cifrado y descifrado se requiere un secreto común, la clave k (Stinson, D. R. (2005)). Tal como se muestra en la Figura 1, la clave es necesaria en los procesos de cifrado y descifrado. Lo cual presenta el problema que corresponde a la distribución de claves. Dicho problema es resuelto con la criptografía asimétrica, la cual establece el uso de clave secreta y pública. En este escenario cada participante tendrá asociado un par de claves (secreta, pública). La clave secreta como su nombre lo indica debe permanecer secreta y la clave pública es conocida por todos los participantes (Rivest, R. L., Shamir, A., & Adleman, L. (1978)), (ElGamal, T. (1985)). Entre este par de claves existe una relación matemática que permite obtener la clave pública a partir de la clave secreta (función de un solo sentido) y es imposible al contrario, obtener la clave secreta a partir de la clave pública (Paar, C., & Pelzl, J. (2009)).

Figura 1. Proceso de cifrado y descifrado simétrico



TRABAJOS RELACIONADOS

Un propuesta para el uso de un procedimiento clásico de cifrado corresponde al trabajo denominado *Substitution & transposition on images by using advanced affine cipher* (Benlcouiri, Y., Ismaili, M. C., & Azizi, A. (2014, April)), el cual propone utilizar el cifrado Afin que demanda un mínimo de recursos para la transferencia de imágenes. Otra propuesta de un procedimiento clásico de cifrado se da en *Reverse Circle Cipher for personal and network security* Isaac, E. R., Isaac, J. H., & Visumathi, J. (2013, February), en el cual se propone utilizar en el proceso de cifrado y descifrado la transposición y substitución polialfabética de Verman. En ambas propuestas se pretende darle una aplicación a los métodos criptográficos clásicos. Los cuales pueden ser una muy buena opción en el fortalecimiento de la seguridad y protección de datos sensibles.

Transposición por Columnas

El proceso de cifrado de este método consiste de los siguientes pasos:

1. Se escribe el texto plano "*en algún lugar de la mancha*", cuya longitud es 27.
2. Se define un número de columnas $\boldsymbol{k} = 6$.
3. Construcción de las columnas

e	n	a	l	g
ú	n	l	u	G
a	r	d	e	
l	a	m	a	N
c	h	a		

4. Ordenamiento de las columnas resultantes para obtener el texto cifrado "*eúalcnnrah aldmldmlueagg n*"

Texto plano "*en algún lugar de la mancha*", texto cifrado "*eúalcnnrah aldmldmlueagg n*".

El proceso de descifrado consiste de los siguientes pasos:

1. Se requiere el texto cifrado "*eúalcnnrah aldmldmlueagg n*".
2. Es necesario el número de columnas utilizado $\boldsymbol{k} = 6$.
3. Se inicia tomando la primera letra del texto cifrado, e y se realiza un desplazamiento de k-1 = 5 para tomar el siguiente carácter, en este caso es n y así sucesivamente. Una vez que se recorrió todo el texto cifrado se avanza con el siguiente carácter del texto cifrado y el proceso finaliza cuando se accede al último carácter.

Texto cifrado "*eúalcnnrah aldmldmlueagg n*", texto plano "*en algún lugar de la mancha*".

Reversa

El proceso de cifrado de este método simple que consiste de los siguientes pasos:

1. Se escribe el texto plano "*en algún lugar de la mancha*".
2. Se obtiene texto cifrado que corresponde a él orden inverso del texto plano "*ahcnam al ed ragul nùgla ne*".

Texto plano "*en algún lugar de la mancha*", texto cifrado "*ahcnam al ed ragul nùgla ne*".

El proceso de descifrado de este método consiste de los siguientes pasos:

1. Se escribe el texto cifrado "*ahcnam al ed ragul nùgla ne*".
2. Se obtiene texto plano que corresponde a él orden inverso del texto cifrado "en algún lugar de la mancha".

Texto cifrado "*ahcnam al ed ragul nùgla ne*", texto plano "*en algún lugar de la mancha*".

Vigenère

Este método criptográfico clásico corresponde a la sustitución polialfabética, fue propuesto por Blaise de Vigenère en 1586. En aquellos años no se le dio especial interés a este método debido al interés centrado en los nomenclátores, que trataban de codificaciones de palabras y frases reemplazadas por números.

Para ilustrar el método de Vigenère es necesario codificar y definir un alfabeto (símbolo-índice):

a-0, b-1, c-2, d-3, e-4, f-5, g-6, h-7, i-8, j-9, k-10, l-11, m-12, n-13, ñ-14, o-15, p-16, q-17, r-18, s-19, t-20, u-21, v-22, w-23, x-24, y-25, z-26, á-27, é-28, í-29, ó-30, ú-31, espacio-32

El alfabeto tiene una longitud $\boldsymbol{n} = 33$.
Proceso de cifrado:

1. Se escribe el texto plano "*en algún lugar de la mancha*".

2. Se elige una palabra clave, para este caso "*claves*" con longitud t=6.
3. Para cada carácter del texto plano se realiza la siguiente operación matemática:

$$y(i) = (x(i) + c(i \bmod t)) \bmod n$$

Donde $y(i)$ corresponde al i-ésimo carácter del texto cifrado, $x(i)$ es el i-ésimo carácter del texto plano, $c(i \bmod t)$ carácter de la palabra clave, n longitud del alfabeto, t longitud de la clave y mod operación modulo.

Ejemplo: $n = 33$ y $t = 6$

Tabla 1. Ejemplo del proceso de Cifrado con Vigenère.

i	Texto Plano	índice	Clave	Índice	$y(i) = (x(i) + c(i \bmod t)) \bmod n$	Texto Cifrado
0	*e*	4	*c*	2	6	*g*
1	*n*	13	*l*	11	24	*x*
2		32	*a*	0	32	
3	*a*	0	*v*	22	22	*v*
4	*l*	11	*e*	4	15	*o*
5	*g*	6	*s*	19	25	*y*
6	*ú*	31	*c*	2	0	*a*
7	*n*	13	*l*	11	24	*x*
8		32	*a*	0	32	
9	*l*	11	*v*	22	0	*a*
10	*u*	21	*e*	4	25	*y*
11	*g*	6	*s*	19	25	*y*
12	*a*	0	*c*	2	2	*c*
13	*r*	18	*l*	11	29	*í*
14		32	*a*	0	32	
15	*d*	3	*v*	22	25	*y*
16	*e*	4	*e*	4	8	*g*
17		32	*s*	19	18	*r*
18	*l*	11	*c*	2	13	*n*
19	*a*	0	*l*	11	11	*l*
20		32	*a*	0	32	
21	*m*	12	*v*	22	1	*b*
22	*a*	0	*e*	4	4	*e*
23	*n*	13	*s*	19	32	
24	*c*	2	*c*	2	4	*e*
25	*h*	7	*l*	11	18	*r*
26	*a*	0	*a*	0	0	*a*

Texto plano "*en algún lugar de la mancha*", texto cifrado "*gx voyax ayycí ygrnl be era*".

Proceso de descifrado:

1. Se escribe el texto plano "*gx voyax ayycí ygrnl be era*".
2. Se requiere la clave utilizada en el proceso de cifrado, para este caso "claves".
3. Para cada carácter del texto cifrado se realiza la siguiente operación matemática:

$$x(i) = (y(i) - c(i \bmod t)) \bmod n$$

Donde $y(i)$ corresponde al i-ésimo carácter del texto cifrado, $x(i)$ es el i-ésimo carácter del texto plano, $c(i \bmod t)$ carácter de la palabra clave, n longitud del alfabeto, t longitud de la clave y mod operación modulo.

Ejemplo: $n = 33$ y $t = 6$

Tabla 2. Ejemplo del proceso de descifrado con Vigenère. Texto cifrado "*gx voyax ayycí ygrnl be era*", texto plano "*en algún lugar de la mancha*".

i	Texto Cifrado	índice	Clave	Índice	$x(i) = (y(i) - c(i \bmod t)) \bmod n$	Texto Plano
0	g	6	c	2	4	e
1	x	24	l	11	13	n
2		32	a	0	32	
3	v	22	v	22	0	a
4	o	15	e	4	11	l
5	y	25	s	19	6	g
6	a	0	c	2	31	ú
7	x	24	l	11	13	n
8		32	a	0	32	
9	a	0	v	22	11	l
10	y	25	e	4	21	u
11	y	25	s	19	6	g
12	c	2	c	2	0	a
13	í	29	l	11	18	r
14		32	a	0	32	
15	y	25	v	22	3	d
16	g	8	e	4	4	e
17	r	18	s	19	32	
18	n	13	c	2	11	l
19	l	11	l	11	0	a
20		32	a	0	32	
21	b	1	v	22	12	m
22	e	4	e	4	0	a
23		32	s	19	13	n
24	e	4	c	2	2	c

25	r	18	l	11	7	h
26	a	0	a	0	0	a

Con el método de Vigenère, se logra perder la estadística que se presenta en la sustitución monoalfabética.

Cryptool

Es un software de criptografía y de criptoanálisis propuesto desde el año de 1998 para fines de aprendizaje que soporta seis idiomas (Alemán, Inglés, Español, Polaco, Serbio, y Francés). Este software está disponible sólo para la plataforma de Windows (https://www.cryptool.org/en/ctp-cryptoolportal-home) y ofrece las siguientes opciones:

- ✓ El cifrado y descifrado con varios algoritmos clásicos y modernos.
- ✓ Verificación de la operación de algunos algoritmos clásicos y modernos (Cesar, Enigma, RSA, etc.)
- ✓ Criptoanálisis de algunos algoritmos (Vigenère, RSA, AES, etc.)
- ✓ Tutorial sobre Teoría de Números.

Son varias las Instituciones que realizan las contribuciones para el crecimiento y mejoramiento de Cryptool:

- ✓ University of Siegen, Germany
- ✓ University of Duisburg-Essen, Germany
- ✓ Ruhr-Universität Bochum, Germany
- ✓ Universität Kassel
- ✓ Deutsche Bank AG
- ✓ Technische Universität Darmstadt, Germany
- ✓ Center of Advanced Security Research Darmstadt (CASED)
- ✓ Politechnika Warszawska, Poland
- ✓ Consejo Superior de Investigaciones Científicas, Spain
- ✓ Klagenfurt University, Austria
- ✓ FH Oberösterreich, Campus Hagenberg
- ✓ University of Singidunum, Serbia

GnuPG (GPG).

Gnu Privacy Guard (Gnupg.org. (2017)) es otro ejemplo de software criptográfico de código abierto desarrollado para ser utilizado en las comunicaciones seguras (https://www.gnupg.org). Este proyecto nace en el año de 1997 gracias a un fuerte apoyo económico realizado por el gobierno de Alemania. Actualmente GPG es una de las herramientas criptográficas más utilizadas en el mundo para cifrar y descifrar datos mediante algoritmos criptográficos simétricos, asimétricos y firma digital. Una de las desventajas que se pueden resaltar al utilizar este software es la inserción de firmas representativas de el o los algoritmos utilizados en el proceso de cifrado. Los algoritmos disponibles en GPG son:

Simétricos

- ✓ -AES, 3DES, TwoFish, BlowFish, Camellia

Asimétricos

- ✓ RSA, ElGamal

Propuesta Criptográfica Basada en Métodos Clásicos
Este trabajo propone el uso recurrente a elección del usuario de los métodos clásicos de cifrado transposición por columnas, reversa y Vigenère. Esta propuesta generara una clave correspondiente a un archivo que tenga la especificación del orden y especificación de los métodos utilizados.

Identificación de transposición columnar:

T Número_de_columnas
Ejemplo: T 749
Indica que al texto plano se le aplicó una transposición de 749 columnas.

Identificación de Reversa:

R, indica que al texto plano se le aplico el procedimiento de reversa.

Identificación de Vigenère:

EV elemento1 de la clave, elemento2 de la clave,…, elemento t de la clave.

Ejemplo:
EV 130,164,178,113,191,197,218,77,25,235,161,157

Indica que el texto plano fue cifrado mediante el método de Vigenère y la clave conformada por los elementos
130,164,178,113,191,197,218,77,25,235,161,157.

Vigenère nos permite una variante adicional que se puede aplicar al texto plano, la cual corresponde al proceso de descifrado. Es decir, el texto plano puede ser cifrado o descifrado con el método de Vigenère.

DV elemento1 de la clave, elemento2 de la clave, …, elemento t de la clave.

Ejemplo:
DV 130,164,178,113,191,197,218,77,25,235,161,157

Indica que el texto plano fue descifrado mediante el método de Vigenère y la clave conformada por los elementos
130,164,178,113,191,197,218,77,25,235,161,157.

Ejemplo del proceso de cifrado y descifrado

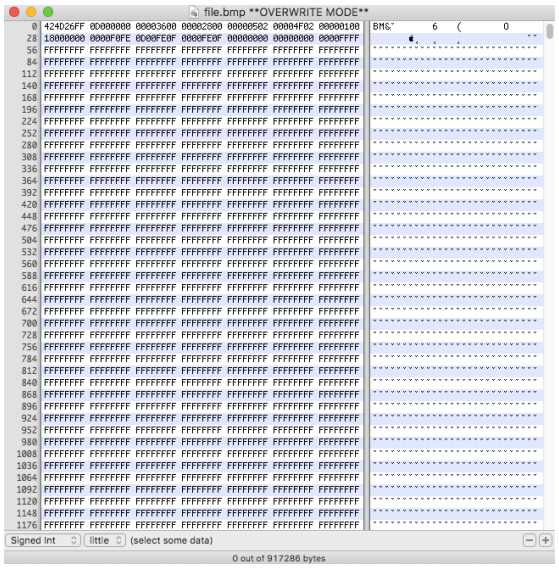
Cifrado:
T 345
T 1032
R
T 925
DV 34,23,67,135,99,242,77,32
EV 130,164,178,113,191,197,218,77,25,235,161,157
R
T 1024
Esta especificación que corresponde a la combinación de los métodos clásicos, indica que al texto plano se le aplicó de manera secuencial 1) transposición de 345 columnas, 2) transposición de 1032 columnas, 3) reversa, 4) transposición de 925 columnas, 5) descifrado de Vigenère con la clave 34,23,67,135,99,242,77,32, 6) cifrado de Vigenère con la clave 130,164,178,113,191,197,218,77,25,235,161,157, 7) reversa, 8) transposición de 1024 columnas.

Descifrado:
El proceso de descifrado debe aplicarse en el orden inverso de cifrado.
T 1024
R
DV 130,164,178,113,191,197,218,77,25,235,161,157
EV 34,23,67,135,99,242,77,32
T 925
R
T 1032
T 345
Esto indica que al texto cifrado se debe aplicar de manera secuencial 1) transposición inversa de 1024 columnas, 2) reversa, 3) descifrado de Vigenère con la clave 130,164,178,113,191,197,218,77,25,235,161,157, 4) cifrado de Vigenère con la clave 34,23,67,135,99,242,77,32, 5) transposición inversa de 925 columnas, 6) reversa, 7) transposición inversa de 1032 columnas, 8) transposición inversa de 345 columnas.

PRUEBAS REALIZADAS

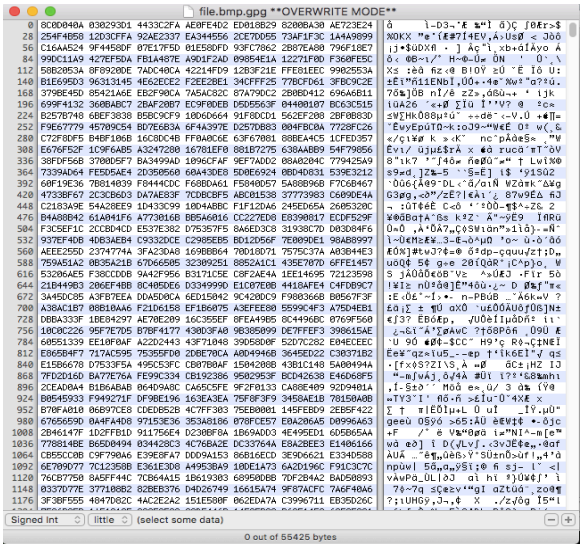
Una de las pruebas realizadas fue sobre un archivo de imagen en formato bmp, de tamaño 917286 bytes, dimensiones 517 x 591, espacio de color RGB. Esta imagen presenta una amplia concentración del color blanco, tal como puede observarse en la Figura 2, que muestra los primeros 1204 bytes.

Figura 2. Primeros 1024 bytes de la imagen de prueba.



En la Figura 3, se muestran los primeros 1024 bytes cifrados con la GPG y el algoritmo Blowfish. Como puede observarse los patrones repetitivos del color blanco ya no se encuentran presentes.

Figura 3. Primeros 1024 bytes de la imagen de prueba cifrada con el software

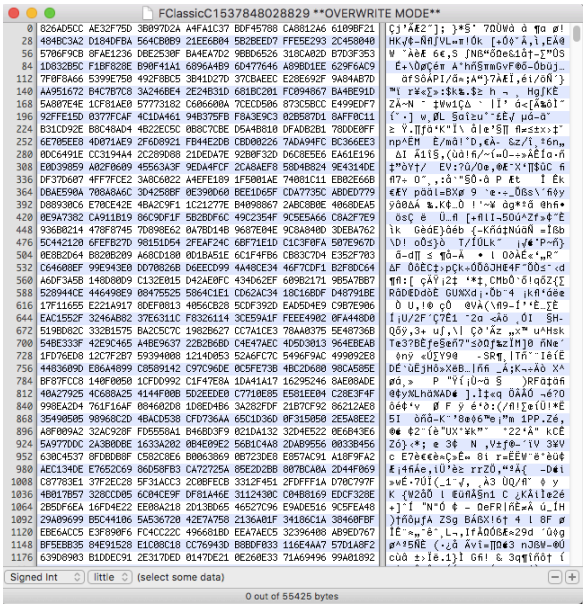


GPG y el algoritmo Blowfish, k =”holamundo”.

En la Figura 4, se muestran los primeros 1024 bytes resultantes de cifrar el archivo de la Figura 3 con el procedimiento propuesto y la siguiente especificación de clave:
T 345, T 1032, R, T 925, DV 34,23,67,135,99,242,77,32,
EV
130,164,178,113,191,197,218,77,25,235,161,157, R, T 1024

Un criptoanalista necesitara romper primero los procedimientos clásicos para obtener el cifrado de GPG y Blowfish. Gracias a esto se logra un aumento en el atributo de confidencialidad, logrando una mayor privacidad de los datos.

Figura 4. Primeros 1024 bytes del cifrado con GPG y el algoritmo Blowfish, k =”holamundo”, y el Procedimiento propuesto con clave T 345, T 1032, R, T 925, DV 34,23,67,135,99,242,77,32, EV 130,164,178,113,191,197,218,77,25,235,161,157, R, T 1024.



CONCLUSIONES

La sociedad requiere de procedimientos criptográficos que garanticen la privacidad de sus datos sensibles. Los sistemas criptográficos modernos pueden ser usados en combinación con los métodos clásicos de cifrado para obtener una mejor confidencialidad de los datos. De esta propuesta se concluye que al utilizar los procedimientos clásicos se agrega una mayor incertidumbre en el contenido cifrado, en particular con los métodos transposición columnar, reversa y Vigenère. Se recomienda utilizar una clave larga con el método de Vigenère, ya que este método aplicado con una clave corta pondrá en evidencia en patrones repetitivos en el texto cifrado caso de existir patrones repetitivos en el texto plano.

REFERENCIAS

STINSON, D. R. (2005). *CRYPTOGRAPHY: THEORY AND PRACTICE*. CRC PRESS.

PAAR, C., & PELZL, J. (2009). *UNDERSTANDING CRYPTOGRAPHY: A TEXTBOOK FOR STUDENTS AND PRACTITIONERS*. SPRINGER SCIENCE & BUSINESS MEDIA.

SWENSON, C. (2008). *MODERN CRYPTANALYSIS: TECHNIQUES FOR ADVANCED CODE BREAKING*. JOHN WILEY & SONS.

MENEZES, A. J., VAN OORSCHOT, P. C., & VANSTONE, S. A. (1996). *HANDBOOK OF APPLIED CRYPTOGRAPHY*. CRC PRESS.

GNUPG.ORG. (2017). THE GNU PRIVACY GUARD. [EN LÍNEA] DISPONIBLE EN: HTTPS://GNUPG.ORG/ [ACCESO 11 OCT. 2017].

ELGAMAL, T. (1985). A PUBLIC KEY CRYPTOSYSTEM AND A SIGNATURE SCHEME BASED ON DISCRETE LOGARITHMS. IEEE TRANSACTIONS ON INFORMATION THEORY, 31(4), 469-472.

RIVEST, R. L., SHAMIR, A., & ADLEMAN, L. (1978). A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEMS. COMMUNICATIONS OF THE ACM, 21(2), 120-126.

BENLCOUIRI, Y., ISMAILI, M. C., & AZIZI, A. (2014, APRIL). SUBSTITUTION & TRANSPOSITION ON IMAGES BY USING ADVANCED AFFINE CIPHER. IN MULTIMEDIA COMPUTING AND SYSTEMS (ICMCS), 2014 INTERNATIONAL CONFERENCE ON (PP. 1256-1259). IEEE.

ISAAC, E. R., ISAAC, J. H., & VISUMATHI, J. (2013, FEBRUARY). REVERSE CIRCLE CIPHER FOR PERSONAL AND NETWORK SECURITY. IN INFORMATION COMMUNICATION AND EMBEDDED SYSTEMS (ICICES), 2013 INTERNATIONAL CONFERENCE ON (PP. 346-351). IEEE.