التعويض الهجائي الاحادي Monoalphabetic Substitution

عندما تستخدم انظمة التشفير شفرة هجائية وحيدة لغرض التعويض، فانها تدعى بشفرات التعويض الهجائي الاحادي (monoalphabetic substitution ciphers). ان كافة التعويضات الهجائية التي تم التطرق اليها لحد الان هي من النوع الهجائي الاحادي، اي انها تستخدم شفرة هجائية واحدة.

ان عملية التشفير باستخدام الشفرة القيصرية يمكنها توليد (25) هجائية من التعويض الهجائي الاحادي. هذه الهجائيات موضحة في الشكل (16 - 4) وهي نتيجة للبرنامج المبين في الشكل (17 - 4).

لاتستطيع الشفرات القيصرية التعويضية ان توفر لنا نصاً مشفوراً ذا امنية عالية، مع ذلك فان مثل هذه النصوص المشفورة غير قابلة للحل حين قراءتها. ولكن، في حالة تمييز وجود ازاحة في مواضع الاحرف، فمن الممكن اشتقاق المفتاح ومن ثم قراءة النص المشفور. إن احد المساوىء الكبيرة في منطوق الامنية للشفرة القيصرية هو حقيقة وجود ازاحة ثابتة (fixed displacement) او تزحيف في الاحرف. مثل هذه المساوىء يمكن تلافيها في بعض انظمة التشفير المذكورة لاحقا.

الشفرات الهجائية العشرية Decimated Alphabet Ciphers

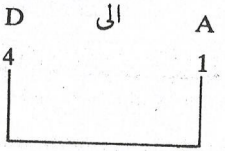
ان هجائية الشفرة القيصرية تحتوي على ازاحة ثابتة تعتمد على مفتاح وتكون الاحرف فيها ذات تسلسل متتابع. ولضمان توفير امنية عالية ينبغي ايجاد هجائية تستخدم مفتاحاً يقوم بتوفير الازاحة ولكن بشرط ان تكون الاحرف فيها ذات تسلسل متتابع. مثل هذه الابجدية من الممكن توفيرها بواسطة نظام الشفرة العشرية(decimated cipher system).

في الشفرة القيصرية تمت اضافة قيمة وحيدة للمفتاح تتراوح بين (1) الى (26) الى الهجائية الاصلية لتوليد الازاحة وهجائية النص المشفور الناتجة. وان الافضل من اضافة المفتاح هو استخدام مضاعف لغرض توليد الهجائية العشرية (decimated alphabet). لغرض توضيح عملية توليد هجائية الشفرة العشرية، سوف تستخدم مفتاح ذو قيمة (K = 3). ان عملية تطوير التسلسل المتتابع للشفرة القيصرية والتسلسل غير المتتابع للشفرة العشرية هي كالاتي:

1 - تسلسل متتابع ـ الشفرة القيصرية، K = 3

النص الصريح	A	B	C	D	E	F	. . .	U	V	W	X	Y	Z
(رقما)	1	2	3	4	5	6	. . .	21	22	23	24	25	26
النص المشفور	D	E	F	G	H	I	. . .	X	Y	Z	A	B	C
(رقما)	4	5	6	7	8	9	. . .	24	25	26	1	2	3

الازاحة من حرف الى حرف هي ثابتة :



الاحرف . . . DEF متتابعة .

2 - تسلسل غير متتابع ـ شفرة عشرية، k = 3

النص الصريح	A	B	C	D	E	F	. . .	U	V	W	X	Y	Z
(رقما)	1	2	3	4	5	6	. . .	21	22	23	24	25	26
النص المشفور	C	F	I	L	O	R	. . .	K	N	Q	T	W	Z
(رقما)	3	6	9	12	15	18	. . .	11	14	17	20	23	26

الازاحة من حرف الى حرف غير ثابتة

A الى C = 1 الى 3
B الى F = 2 الى 6
Y الى W = 25 الى 23

ان نمط الاحرف غير متتابع وهجائية المشفور تتألف من كل حرف ثالث من هجائية النص الصريح .
تم اعادة ترتيب كافة احرف هجائية النص الصريح .
لغرض توليد الهجائية العشرية، تستخدم الطريقة الاتية :-

1 - خذ كل من احرف الابجدية الاعتيادية واستبدله بقيمة الرقم المقابل له:
$A = 1, B = 2, \ldots, Z = 26$.

2 - خذ كل قيمة عددية واضربها برقم المفتاح (K). من الممكن ان يكون هذا المفتاح اي رقم وتري ،
.(

3 - قسّم نتيجة الخطوة الثانية على الرقم (26.1). خذ جزء العدد الصحيح من خارج القسمة (2,1,0) ثم اضربه بالرقم (26). اطرح القيمة المشتقة من نتيجة الخطوة الثانية.

4 - اشتق هجائية النص المشفور باستخدام مكافئات الحرف للارقام التي تم الحصول عليها في الخطوة الثالثة.

ولاجل توضيح عملية الحصول على هجائية الشفرة العشرية، افرض مايلي:-

a = القيمة العددية لاحرف الهجائية الاعتيادية
K = قيمة المفتاح
$b = Ka / 26.1$
c = القيمة العددية لاحرف الهجائية العشرية

حرف النص الصريح	القيمة العددية (a)	Ka (K=3)	b = (Ka)/26.1	c = Ka − b′(26)	حرف الهجائية العشرية
A	1	3	0.115	3 = 3 − 0 × 26	C
B	2	6	0.230	6 = 6 − 0 × 26	F
C	3	9	0.346	9 = 9 − 0 × 26	I
M	13	39	1.494	13 = 39 − 1 × 26	M
N	14	42	1.609	16 = 42 − 1 × 26	P
X	24	72	2.759	20 = 72 − 2 × 26	T
Y	25	75	2.874	23 = 75 − 2 × 26	W
Z	26	78	2.989	26 = 78 − 2 × 26	Z

شفرة هجائية عشرية جزئياً، قيمة المفتاح $K = 3$

بعدئذٍ،

$$c = K\,a - b'(26)$$

حيث ان (b′) هي جزء العدد الصحيح من القيمة (b) (اي، 0، 1، أو 2).

الهجائية الاعتيادية	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
القيمة العددية (a)	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
K=3, K*a*	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78
c	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	26
المشفور	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z
K=5, K*a*	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	125	130
c	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21	26
المشفور	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G	L	Q	V	A	F	K	P	U	Z
K=9, K*a*	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144	153	162	171	180	189	198	207	216	225	234
c	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17	26
المشفور	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z

) هجائيات الشفرة العشرية، قيم المفتاح (K= 3,5,9.)

ان الطريقة الاعتيادية لكتابة الرسائل تتبع نمط معين من اليسار الى اليمين (بالنسبة للغة الانكليزية) وسطر بعد سطر. الرسائل اذن تشكل (نمط هندسي) على هيئة مستطيل. كل شكل ممكن قراءته وفهمه بسبب كون النمط الهندسي هو نمط قياسي لاغراض ارسال المعلومات المطبوعة. اي نمط هندسي آخر سيؤدي الى تمويه الرسالة، الا في حالة كون القارىء على علم بالمفتاح الذي يستطيع اعادة ترتيبها.

الرسالة، CONCEAL ALL MESSAGES، تشكل خطاً افقياً واحداً يمكن ابدالها الى اشكال مستطيلة (1) بهيئة عمودين متساويين في الطول بواسطة كتابة النص الواضح عمودياً:

CL
OM
NE
CS
ES
AA
LG
AE
LS

او (2) بهيئة صفين متساويين في الطول بواسطة كتابة النص الواضح افقياً:

CONCEALAL
LMESSAGES

ان عدد الانماط المستطيلة المختلفة يعتمد على عدد احرف الرسالة اضافة الى حجم الصفحة في الرسالة السابقة، كان هنالك 18 حرفاً يمكن تحويلها الى اربعة مستطيلات: 9 × 2 و 2 × 9، أو كما مبين ادناه، 3 × 6 و 6 × 3.

CON	CONCEA
CEA	LALLME
LAL	SSAGES
LME	
SSA	
GES	

ان عملية ابدال النص الصريح باستخدام طريقة التشفير المبينة على الاشكال الهندسية فقط تعطي امنية للرسالة ذات درجة محدودة جدا. ولكن هذه الانماط الهندسية تكون ذات فائدة عند استخدامها من حيث كونها مرحلة وسطية لعملية تشفير اخرى تدعى ابدال المسلك التي سيتم شرحها ادناه.

ان طرق ابدال المسلك توفر مزجاً اضافياً للرسائل ذات الاشكال الهندسية. عند توليد الشكل الهندسي نتبع نمط الكتابة من اليسار الى اليمين. طول الرسالة SEND HELP SOON هو 12 حرفاً. لغرض الحصول على نص مشفور هندسي يمكن وضع الرسالة على شكل مستطيل 2 × 6 باتباع المسلك من اليسار الى اليمين مع اخذ حرفين في كل مرة.

النص الصريح SEND HELP SOON

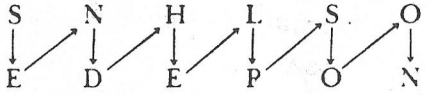
النص المشفور SE
ND
HE
LP
SO
ON

بما ان المسلك من اليسار الى اليمين فان الرسالة سهلة الفهم. وبذلك فان هذه الطريقة توفر امنية قليلة جداً. يمكن الحصول على زيادة في المزج في حالة استخدام الشكل 2 × 6 بصفته مرحلة وسطية يكتب العمود الاولى افقيا من اليسار الى اليمين ثم يكتب العمود الثاني تحته. النتيجة هي ابدال المسلك كما مبين في النص المشفور الاتي:

النص الصريح SEND HELP SOON

النص المشفور SNHLSO
EDEPON

ان هذه الطريقة الشفرية تدعى ابدال المسلك المتعرج (zig-zag) او شفرة السياج المقضب (rail fence). يقسم النص الصريح الى اطوال ثابتة. احد الاطوال يحوي على كل حرف وتري الموقع من الرسالة. الطول الاخر يحوي كل حرف شفعي الموقع. ان عملية الابدال تتبع النمط الاتي ولهذا فان الاسم (المسلك المتعرج) يطلق عليها:

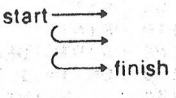


برنامج تشفير الرسائل باستخدام طريقة ابدال المسلك المتعرج المبين في الشكل (5 - 3). يتم ترتيب البرنامج لرسالة طولها 12 حرفاً. في حالة وجود رسائل اطول فيجب اعادة النظر في ايعاز (DIMENSION السطر 15) وكذلك ايعاز (FOR السطران 25 و60). لايمكن لطول الرسالة ان يتجاوز ضعفي عرض الورقة المستخدمة للخارج.

ابدالات المسلك ممكن ان تأخذ اتجاهات متعددة ومختلفة : افقي ، عمودي ، خط قطري ، مع عقرب الساعات او عكس عقرب الساعات . فاذا استخدمنا الرسالة SEND HELP SOON بشكل هندسي 4 × 3، يمكننا توضيح عدد من ابدالات المسالك وكما يلي :

المسالك الافقية

(1) SEND
HELP
SOON



(2) NOOS
PLEH
DNES

المسالك العمودية

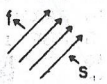
(1) SDLO
EHPO
NESN

(2) NSEN
OPHE
OLDS

المسالك القطرية

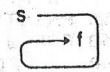
(1) SEDL
NHPO
ESON

(2) NOSE
OPHN
LDES

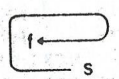


مسالك باتجاه عقرب الساعة (حلزونية)

(1) SEND
OONH
SPLE

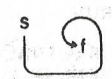


(2) ELPS
HNOO
DNES

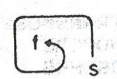


مسالك باتجاه عكس عقرب الساعة

(1) SOSP
EONL
NDHE



(2) EHDN
LNOE
PSOS



Columnar Transposition

الابدال العمودي

التشفير بطريقة الابدال العمودي تحتاج الى ازاحة اعمدة الرسالة ذات النص الصريح والتي هي اصلاً مرتبة على نمط الشكل الهندسي للمستطيل. بصورة عامة، يوضع النص الصريح على شكل مستطيل يتبع المسلك العمودي (1). ابدأ بالرسالة:

SHIP EQUIPMENT ON THE FOURTH OF JULY

يجب اتخاذ القرار بخصوص قياس (الصفوف والاعمدة) للمستطيل المطلوب استخدامه. الرسالة السابقة تحتوي على (30) حرفا ومن الممكن ان تأخذ الاشكال التالية 2×15, 3×10, 5×6, 6×5 ، 3 × 10 و 2×15 في حالة كون الرسالة مؤلفة عدد وتري او عدد لايمكن الحصول منه على شكل هندسي من الاحرف، مثلا (29)، يضاف حرف زائف او ملغي مثل الحرف (X) الى النص الصريح.

اذا اردنا كتابة النص الصريح على شكل ستة صفوف مقابل خمسة اعمدة نحصل على النص المشفور:

ارقام الاعمدة	1	2	3	4	5
النص المشفور	S	U	T	F	O
	H	I	O	O	F
	I	P	N	U	J
	P	M	T	R	U
	E	E	H	T	L
	Q	N	E	H	Y

ان النص المشفور السابق المتمثل في هيئة الابدال العمودي، يمكن قراءته بسهولة وغير قادر على تأمين اية حماية.

لغرض الحصول على زيادة في امنية النص الصريح، يمكن ازاحة الاعمدة في المستطيل 5 × 6 وبذلك نحصل على مايسمى بالابدال العمودي. مثال على ذلك، يمكن ازاحة مواضع الاعمدة 12345 بصورة اعتيادية الى المواضع 34521 التي تعتبر احتمالاً واحداً من مجموع 120 ترتيباً محتملاً*

الابدال العمودي الناتج هو الاتي:

ارقام الاعمدة	3	5	4	2	1
النص المشفور	T	O	F	U	S
	O	F	O	I	H
	N	J	U	P	I
	T	U	R	M	P
	H	L	T	E	E
	E	Y	H	N	Q

يمكننا الحصول على تحسينات اضافية لامنية النص الصريح عند تدوين الرسالة التي تم ابدالها على هيئة مجاميع ذات خمسة احرف مأخوذة افقياً من المستطيل وبذلك نحصل على النص المشفور النهائي:

النص الصريح SHIP EQUIPMENT ON THE FOURTH OF JULY

النص المشفور TOFUS OFOIH NJUPI TURMP HLTEE EYHNQ

ويمكن استغمال اسلوبا بديلاً بأخذ الحروف من المستطيل على شكل مسلك عمودي وهذا ينتج النص المشفور الاتي مدوناً على شكل مجاميع ذات خمسة حروف:

النص الصريح SHIP EQUIPMENT ON THE FOURTH OF JULY

النص المشفور TONTH EOFJU LYFOU RTHUI PMENS HIPEQ

النصوص المشفورة عمودياً لايمكن قراءتها بسهولة دون معرفة القارىء بعض المعلومات عن طريقة التشفير المستخدمة. يجب على مستلم النص المشفور ان تكون لديه المعلومات المحددة الاتية:

1 - يجب ان يعرف كيف تم اخذ النص المشفور من الشكل الهندسي، اما افقياً او عمودياً او قطرياً او غير ذلك.

2 - يجب ان يعرف عدد الصفوف والاعمدة للمستطيل.

3 - يجب ان يعرف المفتاح. ومعنى ذلك، ان اعمدة المستطيل اعيد ترتيبها وفق مفتاح رقمي (number key)، مثال على ذلك 35421. يجب على كل من المرسل والمستلم معرفة هذا المفتاح.

والشكل (10 - 3) عبارة عن برنامج يتعامل مع النص الصريح على هيئة ابدال المستطيل، يقوم بابدال الاعمدة ثم ينتج النص المشفور النهائي بصورة افقية.

---

* هنالك عدد (C) من العوامل (C!) المحتملة للابدالات العمودية للقيمة (C) تساوي خمسة اعمدة؛ اي ان، (ترتيب) 120 = 1 × 2 × 3 × 4 × 5 = 5!