نقاط ضعف نظام شفرة الكتاب

قاسم محمد حسين

كلية علوم الحاسوب والرياضيات ، جامعة تكريت ، تكريت ، العراق

(تاريخ الاستلام: 17 / 2 / 2013 ---- تاريخ القبول: 17 / 3 / 2013)

الملخص

يتناول البحث تحديد نقاط الضعف في نظام التشفير الذي يستخدم حروف كتاب معين كمفاتيح في عملية التشفير وفك التشفير. اعتمد البحث دراسة التوزيع التكراري لحروف النص المشفر وحروف اللغة المستخدمة في كتابة الكتاب وكذلك حروف اللغة المستخدمة في كتابة النص الصريح ، واخذ بنظر الاعتبار استخدام اللغة الانكليزية في كتابة النص الصريح والمفتاح والنص المشفر. استطاع البحث ان يحدد عدد من الثغرات التي يمكن استثمارها في تقليل فضاء المفتاح وتقليل عدد الاحتمالات عند مهاجمة الرسائل المشفرة في هذا النظام. فعلى سبيل المثال ،توجد امكانية لاختصار عدد احتمالات حروف الاعمدة الثلاث الاولى من 17576 استخدم 2475احتمال من 17576 وبنسبة 90،9% . والعلاقة بين حروف الاعمدة قلص الاحتمالات بين 50% الى 73%.. بالاضافة الى تقليص احتمالات حرف النص الصريح لحرف النص المشفرالمشفر بحدود 50%.

كلمات مفتاحية: نظام شفرة الكتاب ، خواص النص المشفر لنظام شفرة الكتاب ، نقاط الضعف في النظام.

1- المقدمة

يختص علم التشفير بدراسة امنية المعلومات . ويتضمن فرعين رئيسيين هما التشفير وتحليل التشفير. يستخدم التشفير دوال رياضية لتشفير الرسائل ، من اجل ضمان حماية معلوماتها السرية، والتي تنقل او تحفظ عبر قنوات غير امينة ، لضمان عدم الاطلاع عليها من المتطفلين والمخربين واللصوص. وتستخدم المفاتيح في تشفير الرسالة (encryption) وفك تشفيرها (decryption). اما تحليل الشفرة (Cryptanalysis) فيقصد به استخدام الاساليب الرياضية والاحصائية للوصول الى النص الصريح او المفتاح ، بدون معرفة مفتاح التشفير .[1]

تعتمد قوة نظام التشفير على طريقة توليد المفتاح (اي الخوارزمية المستخدمة في توليد المفتاح) والتي يجب ان يكون فيها المفتاح عشوائي مع طول كبير له يضمنعدم تكرار ه عند الاستخدام . ان تحقق ذلك يحتاج الى استخدام خوارزميات معقدة تحتاج الى بعض المتطلبات التي تختلف من خوارزمية لاخرى. وكلما كانت الخوارزمية قوية اصبحت مهمة محلل الشفرة اصعب لان الفضاء الذي سيبحث فية سيكون واسعا. [2]

ولقد استخدمت خوارزميات تشفير متنوعة من حيث فلسفة عملها وعدد مفاتيحها ، كما تتباين هذه الخوارزميات من حيث امنيتها (صعوبة مهاجمتها) والمستلزمات التي تحتاجها من قدرات حسابية والوثائق التي يحتاجها المستخدم وتوفر البيئة المناسبة لعملها.

يقوم محلل الشفرة بعملية الهجوم علىنظام التشفير اعتمادا على نوعية خوارزميته وبعض المعلومات التي يحصل عليها والمتعلقة بخواص النص الصريح او حتى العلاقة بين النص الصريح والمشفر. ان المهاجم اما يستثمر نقاط ضعف الخوارزمية لتقليل احتمالات النص الصريح او فضاء المفتاح ، او الهجوم الشامل (Brute force) الذي يأخذ فيه جميع الاحتمالات الممكنة للحل .[1]

وفي بعض الاحيان يكون من الصعوبة توفير مستلزمات نظام التشفير اما لكلفتها او لعدم توفر البيئة الملائمة لاستخدامها كالاجراءات الامنية المتبعة في مكان تواجد مستخدم التشفير. لذا يتم اللجوء الى انظمة تحتاج الحد الادنى من المتطلبات ومن هذه الانظمة الشفرية المستخدمة هو نظام شفرة الكتاب[3] ، وهو نظام يستخدم مفتاح سري متناظر (Symmetric) ذو امنية عالية ،حيث يولد مفتاح تشفير ذو عشوائية عالية يصعب التكهن بها وكذلك ضمان عدم تكرار المفتاح بشكل عام. كما انه لايحتاج الى متطلبات كثيرة من اجهزة او معدات او تبادل مفاتيح او الاحتفاظ بوثائق عند المستخدم . يعتمد هذا النظام على استخدام حروف الكلمات في نص كتاب متوفر في البيئة التي يعمل فيها مستخدم الشفرة كمفاتيح تشفير، ضمن اتفاق متبادل مع مرجعه عن كيفية انتقاء حروف المفتاح. حيث يشفر كل حرف من النص الصريح باستخدام حرف كمفتاح من الكتاب ليولد حرف واحد مشفر ، اي ان طول النص المشفر يساوي طول المفتاح ويساوي طول النص الصريح. ان توليد مفتاح التشفير في هذا النظام يقترب من نظام استخدام المفتاح لمرة واحدة (One time pad).

وعلى الرغم من ان هذه الشفرة ذات امنية عالية كون فضاء المفتاح كبير قدره 26 طول النص الصريح (26 مرفوع الى اس يمثل طول النص الصريح) ، الا انه هنالك بعض نقاط الضعف التي يمكن ان تستثمر في تقليل فضاء المفتاح وبالتالي المساعدة في مهاجمة هذا النظام. وقد بينت بعض المنشورات عن ان هنالك تباين في التوزيع التكراري للحروف حسب موقعها في الكلمة ولكنها لم توضح تفصيليا مقدارهذا التباين او كيفية الاستفادة منه [4][5]، كما لم تؤشر وجود دراسات عن نقاط ضعف امكن تشخيصها بالاعتماد على النص المشفر.

يتناول هذا البحث دراسة نقاط الضعف في نظام شفرة الكتاب من خلال اجراء دراسات على التوزيع التكراري لحروف المفتاح و كذلك دراسة الثغرات التي يمكن معرفتها من دراسة حروف النص المشفر فقط ، و اخذ بنظر الاعتبار استخدام اللغة الانكليزية في كتابة النص الصريح والمفتاح والنص المشفر .

2- نظام شفرة الكتاب

يعتمد هذا النظام على استخدم حروف كلمات النص المكتوب في الكتاب كمفتاح لتشفير الرسائل ذات المحتوى السري ويفضل استعماله عندما يعمل مستخدمها في ظروف تكون من الصعوبة عليه الاحتفاظ بوثائق تشير الى استخدامه لعملية التشفير. حيث ان هذه الشفرة لا تحتاج الى اي وثائق . كما انها لا تحتاج الى تبادل للمفاتيح الشفرية السرية . حيث ان عملية تبادل المفاتيح من المهام الصعبة لما تحتاجه من سرية في تبادلها وتوفير مكان امن سري لحفظها.

ولاجل استخدام شفرة الكتاب لابد ان يتفق طرفي الاتصال ، المرسل والمستلم ، على الاتي: [1][6][7]

1. اختيار كتاب متوفر وشائع الاستخدام في بيئة عمل الشخص السري ، ويكون لدى الطرفين نفس الكتاب من حيث جهة الطبع وسنة الطبع وكذلك الطبعة من اجل ضمان التطابق لمواقع الكلمات والحروف في نصي النسختين .
2. الاتفاق على تسلسل استخدام صفحات الكتاب ، وعلى طريقة تعريف الصفحة التي سيتم اختيار حروف المفاتيح منها. فمثلا يذكر اول واخر حرف من الصفحة في مكان متفق عليه ضمن الرسالة المشفرة ، كأن يكون في بداية الرسالة او في نهايتها. ويجب عدم اختيار هذين الحرفين ضمن المفتاح.
3. الاتفاق على طريقة اختيار الحروف التي ستستخدم كمفاتيح للتشفير ضمن الصفحة. هنالك عدة اتجاهات في كيفية اختيار الحروف ، اسهلها ان تستخدم حروف الاسطر واحدا بعد الاخر (اي بشكل افقي) حيث يستخدم السطر كاملا ثم ينتقل الى السطر الذي يليه ، او ان يتم اختيار حروف من اعمدة محددة في الصفحة . فعلى سبيل المثال استخدام الحرف الاول من كل سطر في الصفحة وبعدها ينتقل الى الحرف الثاني من كل سطر وهكذا ، اي الاستخدام العمودي . وقد يتم الاكتفاء بثلاث اعمدة من الصفحة وفي حالة حالة عدم كفاية حروف تلك الصفحة ، ينتقل الى الاختيارالى الصفحة التالية.
4. الاتفاق على جدول يستخدم لتقاطع المفتاح مع النص الصريح لتوليد النص المشفر عند التشفير ، وتقاطع المفتاح مع النص المشفر لايجاد النص الصريح ، حيث يحتوي الجدول على ابجدية اللغة . ومن امثلة ذلك جدول فيجنر (Vigenere table) او جدول بيفورت. فعلى سبيل المثال لو اردنا تشفير حرف النص الصريح X باستخدام حرف المفتاح R اعتمادا على جدول فيجنر[1] ، فان حرف النص المشفر سيكون هو O . او استخدام جدول خاص يتم بناءه من قبل مصمم الشفرة.

2-1 خواص الشفرة التي تستخدم الكتاب كمفاتيح تشفير.

يمتاز النص المشفر الناتج من استخدام نظام التشفير الذي يستخدم حروف كتاب كمفاتيح للتشفير، بالميزات التالية.

1. عدد حروف النص الصريح والنص والمشفر والمفتاح تكون بنفس العدد.
2. ان اختيار حروف المفتاح يكون عشوائيا ، كونه يعتمد على طبيعة موضوع الكتاب والكلمات المستخدمة فيه. وتكون احتمالية الحرف هو N ، حيث تمثل N عدد حروف ابجدية اللغة المستخدمة في كتابة الكتاب . فمثلا N= 26 في الكتاب المكتوب في اللغة الانكليزية و N=28 في حالة الكتاب المكتوب باللغة العربية.
3. ان التوزيع التكراري لحروف النص المشفر يكون عشوائيا حيث ان دليل التطابق (index coincidence) يقترب من 0.038 وهذه القيمة تعني ان العشوائية جيدة.
4. لاتوجد فرص لوجود تكرارات في النص المشفر يستفاد منها محلل الشفرة في كسرها.
5. ان احتمالية ايجاد نص صريح لنص مشفر هو N^M حيث M هو عدد حروف ذلك النص.
6. لاتستطيع طرق التحليل المستخدمة في انظمة التشفير متعددة الابجديات من مهاجمة هذا النظام بسبب الفضاء الكبير للمفتاح مالم يستخدم نفس المفتاح اكثر من مرة ، حيث يقترب من نظام استخدام المفتاح لمرة واحدة ، وهو النظام الوحيد الغير قابل للكسر في وقتنا الحاضر وذو امنية عالية ، كون المفتاح من النادر تكراره.

2-2 نقاط الضعف في النظام

على الرغم من ان الرسالة المشفرة الناتجة من استخدام شفرة الكتاب لها خواص عشوائية عالية لان اختيار حروف المفتاح الشفري يكون بشكل عشوائيا وفضاءا كبيرا ، الا ان خواص النص المشفر تتأثر بالخواص الاحصائية للغة المستخدمة في كتابة الكتاب (اي للغة المفاتيح) ، وكذلك اللغة التي يكتب بها النص الصريح . لهذا يمكن لمحلل الشفرة ان يستثمر تلك الخواص في تحليل الرسالة المشفرة ومحاولة ايجاد نصها الصريح.[8]

سيتطرق البحث الى تحديد نقاط ضعف طريقتين من طرق استخدام شفرة الكتاب (على افتراض ان مفتاح التشفير من كتاب مكتوب باللغة الانكليزية وكذلك النص الصريح مكتوب ايضا باللغة الانكليزية) وهما :

1. استخدام حروف السطر باكمله.

تعتمد هذه الطريقة على اختيار سطر بعد اخر في صفحات الكتاب ، واستخدام حروف كل سطر بشكل متتالي. فعلى سبيل المثال لو كان لدينا جزء من احدى صفحات كتاب مكتوب باللغة الانكليزية الموضحة في الشكل رقم (1)

The technological advances witnessed in the computer industry are the result of a long chain of immense and successful efforts made by two major forces. These are the academia, represented by university research centers, and the industry, represented by computer companies. It is, however, fair to say that the current technological advances in the computer industry owe their inception to university research centers. In order to appreciate the current technological advances in the computer industry, one has to trace back through the history of computers and their development. The objective of such historical review is to understand the factors affecting computing as we know it today and hopefully to forecast the

شكل رقم (1): جزء من صفحة كتاب مفتاح التشفير

واردنا تشفير النص التالي المكتوب باللغة الانكليزية " Computer systems " باستخدام جدول فيجينر، فان ذلك يتم كما في الجدول رقم (1):

جدول رقم (1): تشفير نص على مفتاح من احدى الصفحات (من شكل رقم 1)

مفتاح التشفير	C	I	G	O	L	O	S	N	H	C	E	T	H	T
النص الصريح	M	E	T	S	Y	S	R	E	T	U	P	M	O	C
النص المشفر	O	M	Z	G	J	G	E	L	V	Y	I	Q	O	V

حيث تم اختيار مفتاح التشفيرمن السطر الاول ، واخذت حروفه بشكل متسلسل.

ان نقطة ضعف هذه الطر يقة هو ان المفتاح سيتأثر بالتوزيع التكراري لحروف اللغة المكتوب بها الكتاب. ويمكن مهاجمتها اما بالاستفادة من العلاقة والترابط بين حروف النص الصريح وكذلك الترابط بين حروف نص المفتاح (الذي يكون ايضا نصا صريحا) ، او باستخدام توقع كلمات محتملة في النص الصريح او كلمات في المفتاح . ان ظهور نص مقروء في اي منهما سيدقق من خلال وجود نص صريح في الثاني. كذلك فان تقاطع المفتاح مع النص الواضح هو نفسه عند تقاطع النص الواضح مع المفتاح . وعليه فان استخدام هكذا اسلوب سيسهل من عمل محلل الشفرة في مهاجمة هذا النظام وبالتالي التوصل الى النص الذي تم تشفيره . حيث لا يحتاج محلل الشفرة الا لمعرفة ترددات الحروف الاحادية والثنائيةوالكلمات الاكثر تكرارا في اللغة (اي تعويض بسيط).

2. استخدام اعمدة متتالية في الصفحة.

يعتمد هذا الاسلوب على اختيار حروف اعمدة محددة في كل صفحة تستخدم حروفها كمفتاح للتشفير. فعلى سبيل المثال ، لو اخترنا الاعمدة بشكل متسلسل من الصفحة الموضحة في الشكل (1) ، اي نأخذ العمود الاول من كل سطر ثم العمود الثاني من كل سطر .. الخ ، سيكون المفتاح المستخدم هو:

TLARNRCTFHOREOEOHAENEPLSMEC

حيث اخذ الحرف T من السطر الاول ، و L من السطر الثاني و الحرف A من السطر الثالث وهكذا لنهاية الصفحة (جميعها من العمود الاول) ، وبعدها انتقل الى حروف العمود الثاني من السطور.

ويلاحظ ان العمود الاول على الغالب يمثل الحرف الاول من الكلمة ، ويمثل العمود الثاني الحرف الثاني والعمود الثالث هو الحرف الثالث من الكلمة . ويشذ عن ذلك عندما يكون الحرف الاول هو استخدم الضمير I او الحرف A ، حيث يكون الحرف في العمود الثاني هو الحرف الاول من الكلمة. كذلك يحدث عندما يبدأ السطر بأحد الضمائر او حروف الجر التي تتكون من حرفين مثل : WE, TO, ME, AN , …etc ، حيث يكون حرف العمود الثالث هو الحرف الاول من الكلمة. وهذا يزيد من عشوائية المفتاح.

ان المفتاح المتكون يقترب كثيرا من نظام استخدام المفتاح لمرة واحدة ان لم تستخدم نفس الصفحة اكثر من مرة. وهذا الاسلوب لايمكن فيه مهاجمة النص المشفر باستخدام الكلمة المحتملة للمفتاح . كذلك لايمكن الاستفادة من الحصول على كلمة في النص الصريح لمعرفة الحرف التالي في المفتاح في بعض الحالات ، اضافة الى عدم امكانية تدقيق صحة النص الصريح الذي تم الحصول عليه.

لقد تم اجراء دراسات احصائية من قبل الباحث لمعرفة امكانية وجود ثغرات يمكن استثمارها في مهاجمة هذا الاسلوب في التشفير . وتم اجراء الدراسات الاحصائية التالية:

أ. تم در اسة التوزيع التكراري لحروف العمود الاول من الصفحات من خلال نموذج احتوى على 5350 حرف. وتبين ان هنالك تباين في ترددات الحروف ، فمنها ذات ترددات عالية ، وحروف اخرى ذات ترددات قليلة جدا ، كما في الجدول رقم (2). كذلك الامر بالنسبة للعمودين الثاني والثالث.

ملاحظة : قيم الجداول مضروبة في (10^{-2})

جدول رقم (2) : ترددات الحروف للاعمدة 1 و 2 و 3 ($10 x^{-2}$)

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
1st column	7.6	4.9	5.7	3.2	3.1	5.1	1.7	4.7	5.1	0.5	0.3	2.4	3.6
2nd column	10.1	0.3	0.7	0.7	12.8	3.8	0.1	13.5	7.6	0	0	1.9	0.7
3rd column	8.1	1	3	4.7	14.3	1.7	2	0.2	6	0.2	1	3.4	4.2

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1st column	2.1	6.6	5	0.2	3.7	7.6	15.2	1.3	1	5.5	0	0.6	0.1
2nd column	8	15.8	1.4	0	6.7	1.9	2.5	4.8	0.9	0.7	0.8	1.3	0.1
3rd column	5.9	6.9	2.7	0.4	8.1	6.5	7.7	3.1	2	1.2	0.2	1.9	0.2

وتبين ان في العمود الاول ان (15) حرفا مثلت ما نسبته 91.6 % من مجموع استعمال حروف العمود الاول. وكان اكثر الحروف ترددا هو حرف T ثم تلاه حرفي S و A.

اما بالنسبة للعمود الثاني فقد اشترك (11) حرف بنسبة 90.6% من مجموع الحروف التي استخدمت كمفتاح. وكان اكثر الحروف ترددا هو حرف O ثم تلاه حرف H و E. في العمود الثالث ظهر (15) حرفا بنسبة 90.4% من مجموع الحروف. وكان اكثر الحروف ترددا هو حرف E ثم تلاه حرفي R (كما موضح في الشكل رقم 2).

ان هذه النسب توضح انه على الرغم من كبر فضاء المفتاح الا ان هنالك نسبة تصل الى نسبة 48% ذات استخدام محدود. وبالتالي فان هذا يقلل من حجم فضاء المفتاح.

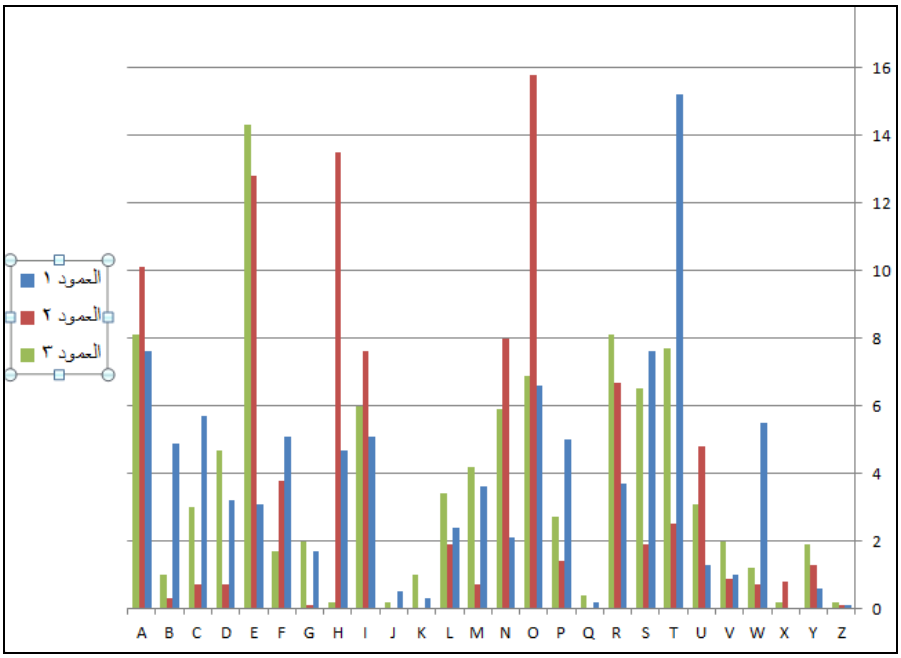
جدول رقم (3) نسب استخدام مجاميع الحروف

العمود المستخدم	عدد الحروف الاكثر استخداما	نسبة استخدامها %	عدد الحروف الاقل او المعدومة الاستخدام	نسبة استخدامها %
الاول	15	91،6	11	8،2
الثاني	11	90،6	15	9،4
الثالث	15	90،4	11	9،6

3. تم دراسة العلاقة الثنائية بين حروف العمود الاول وحروف العمود الثاني ،وتبين ان هنالك (397) احتمال كان ترددها صفر (اي انها لم تظهر لان هذه الحروف لاتأتي متجاورة في الكلمات) من مجموع الاحتمالات الكلية البالغة 2^{26} = 676 احتمال . وهذا سيزيد من نسبة الاحتمالات التي سيهملها محلل الشفرة هو (59%) اي يقلل فضاء البحث. كما موضحة في الجدول رقم (4) .

4. تم دراسة العلاقة الثنائية بين حروف العمود الاول والثالث كانت عدد الاحتمالات التي لم تظهر (496) احتمال كما موضحة في الجدول رقم (5) ، اي بنسبة 73 % ، وهذا سيقلل من فضاء المفتاح.

5. اما العلاقة بين العمودين الاول والثالث فكان لدينا (337) احتمال قيمتها صفر، كما موضحة في الجدول رقم (6). اي ما نسبته (50%).

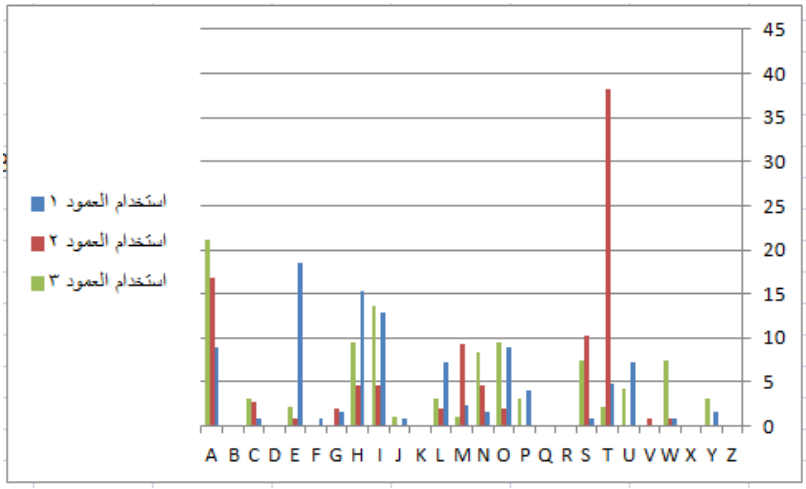


شكل رقم (2): مخطط توزيع الحروف للاعمدة 1 و 2 و3

6. تم تشفير نص طولة 5433 على مفتاح حروفه من احد الاعمدة في كل مرة وتم دراسة احتمالات النص الواضح لكل حرف مشفر ضمن كل عمود على حدة ، وتبين ان كل حرف لا يتولد من جميع الحروف بنفس الكمية ، بل تأثر بالتوزيع التكراري لحروف المفتاح ضمن العمود المختار . حيث تبين من النتائج الموضحة في الجداول (7) و(8) و (9) ، والملخصة في الجدول رقم (10) الاتي:

أ. ان كل حرف مشفر يختلف من حيث توزيعه التكراري من عمود لاخرعند تشفيره . فمثلا لو اخذنا حرف النص المشفر A ، فعندما يكون نتيجة عمليات تشفير باستخدام مفاتيح من العمود الاول فان احتمالية ان يكون حرف النص الصريح له هو الحرف E بنسبة احتمالية 18,5% ، واحتمالية ان يكون حرف النص الصريح هو H بنسبة اختمالية 15,3 %. اما اذا كان الحرف A ناتج من عمليات تشفير مفاتيحها من العمود الثاني فان حرف النص الصريح هو T بنسبة احتمالية 38,3 % وحرف A بنسبة احتمالية 16,8 %. اما اذا كان المفتاح من العمود الثالث فان احتمالية ان يكون النص الصريح هو A كانت 21,1% وان يكون حرف I هي 13,7%. ان التوزيع التكراري لاحتمالات النص الصريح للحرف المشفر A موضحة بالشكل رقم (3). وهكذا بالنسبة لكل حرف من حروف النص المشفر .

ب. تباينت عدد الاحتمالات التي لا تكون فيها حروف محددة مرشحة كحروف نص صريح لحرف معين من حروف النص المشفر من عمود لاخر. فعلى سبيل المثال، لو اخذنا الحرف A فان الحروف B, D, K, Q, U, X, Z مستبعدة ان تكون النص الصريح اذا كان حرف ال A ناتج من استخدام حرف من العمود الاول. وتستبعد الحروف B, D, F, J, K, P, Q, R, U, X, Y, Z . اما اذا كان ناتجا من استخدام مفتاح من العمود الثالث B, D, F, G, K, Q, R, V, X, Z



الشكل رقم (3): احتماليات النص الصريح للحرف A حسب العمود المستخدم

ت. تباينت عدد الاحتمالات لحروف النص الصريح لحروف النص المشفر من حرف لاخر. فعلى سبيل المثال ، ان الحرف A الناتج من استخدام المفتاح الثالث كان هنالك 14 حرف من اصل 26 حرف (وهي حروف الابجدية) مثلت 97،7% من النص الصريح لهذا الحرف ، بينما مثل هذه العدد 100% من الاحتمالات بالنسبة للعمود الثاني.

يلاحظ مما سبق انه اعتمادا على النص المشفريمكن استبعاد حالات من فضاء المفتاح على الرغم من انها تحسب نظريا ، فقد بلغت عدد الاحتمالات التي يمكن الغائها وكما مبينة في الجدول رقم (10) هي 216 و 282و 229 احتمال اذا استخدم المفتاح ، اما العمود الاول والثاني والثالث على التوالي اي يمكن تقليل عدد الاحتمالات بنسبة 32% و 41,7% و 34% على التوالي من فضاء المفتاح اعتمادا على النص المشفر فقط. وبالتالي سيقلل هذا من الجهد الذي يبذله محلل الشفرة في كسر هذا النظام.

3- الاستنتاجات

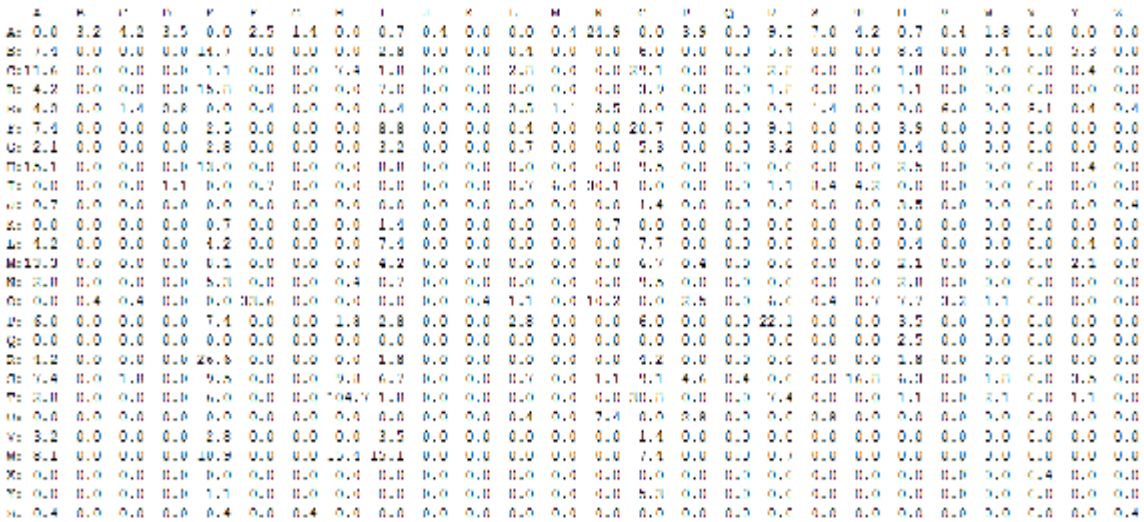
1. ان المفتاح المختار في شفرة الكتاب وان بدا عشوائيا الا انه يتأثر بالتوزيع التكراري لحروف اللغة المستخدمة في كتابة الكتاب المستخدم كمفتاح للتشفير.
2. ان فضاء المفتاح وان بدى كبيرا ، الا انه في واقع الحال اصغر بكثير مما هو فعليا لان التوزيع التكراري لحروف الاعمدة المستخدمة حروفها كمفايتح في عملية التشفير يترك اثره على احتمالات النص الصريح للحرف المشفر. وهذا ما يسهل عملية التعامل معه من قبل محلل الشفرة.
3. ان استخدام جميع حروف السطر بشكل متسلسل ، يمكن مهاجمته بالاستفادة من خواص التوزيع التكراري وكذلك استخدام الكلمات المتوقعة سواء ضمن النص الصريح او ضمن المفتاح الذي يكون صريحا ايضا.
4. ان اضعف الاعمدة عشوائيا هو العمود الثاني لان هنالك حروف لاتظهر وحروف ترددتها عالية.
5. ان استخدام حروف اعمدة متسلسلة في الصفحات ، يمكن ان يستثمر من قبل محلل الشفرة لان ذلك يقلل من فضاء المفتاح ، بسبب عدم ورود عدد من الاحتماليات .
6. ان استخدام حروف اعمدة متباعدة عن بعضها يولد امكانية الخطأ في اختيار المفتاح من قبل المشفر او الذي يحل الشفرة.

4- التوصيات

1. تنفيذ الدراسات الاحصائية التي وردت في هذا البحث على اللغة العربية.
2. استثمار هذه الدراسة في كسر الشفرات التي تستخدم نظام شفرة الكتاب.

الجداول

جدول رقم (4): العلاقة بين العمود الاول والثاني (10×10^{-2})



جدول رقم (5): العلاقة بين حروف العمودين الثاني والثالث (10×10^{-2})

	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:	4.1	0.0	1.1	23.5	7.3	1.2	2.4	0.0	0.4	0.0	0.8	2.8	1.2	0.8	7.7	4.5	0.8	1.2	2.8	6.1	1.2	0.4	0.4	0.0	2.4	0.0
B:	0.0	0.4	1.1	0.4	0.1	0.4	2.4	0.4	0.8	0.0	0.4	2.0	0.0	2.0	8.2	0.8	0.0	0.1	2.0	20.6	1.2	0.0	0.0	0.0	1.2	0.0
C:	6.9	0.0	0.0	0.0	2.0	0.4	0.0	0.0	0.2	0.0	0.0	2.0	12.2	17.6	4.5	1.2	0.0	4.1	7.2	1.6	0.7	0.0	0.0	0.0	0.4	0.0
D:	2.4	0.4	2.0	1.2	1.6	2.4	0.4	0.0	1.6	0.0	0.0	0.0	2.0	1.2	0.0	1.2	0.0	0.4	17.0	4.5	0.4	0.4	0.0	0.0	2.0	0.0
E:	2.0	0.0	2.0	0.4	7.3	0.8	1.2	0.0	4.1	1.2	0.0	0.0	0.4	0.0	3.2	6.9	0.0	1.2	2.4	4.1	0.4	0.0	0.0	0.0	0.0	0.0
F:	2.4	0.0	2.0	0.8	2.4	0.4	0.8	0.0	2.4	0.0	0.4	4.9	1.2	6.9	8.5	0.0	0.0	22.3	0.8	1.2	2.0	0.4	0.0	0.4	0.4	0.0
G:	2.0	0.4	0.0	0.0	0.0	0.0	0.4	0.0	1.6	0.0	0.0	0.0	0.0	0.0	2.7	0.0	0.0	2.0	0.0	2.0	0.0	2.0	0.0	0.0	0.0	0.4
H:	2.0	0.4	0.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	5.7	1.6	0.4	2.0	0.0	6.5	1.2	1.2	2.0	0.1	2.4	0.0	0.0	0.0
I:	2.0	0.0	2.0	1.2	1.2	2.4	0.0	0.4	1.6	0.0	0.0	0.0	0.4	0.4	0.0	4.5	0.0	0.4	4.9	6.5	0.0	0.2	0.0	0.0	0.0	0.0
J:	0.0	1.2	0.0	0.8	0.0	0.0	0.0	0.0	0.8	0.0	0.0	0.0	0.8	0.0	0.0	0.0	0.0	0.0	2.0	0.0	0.8	0.0	0.0	0.0	0.0	0.0
K:	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.2	0.8	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4	0.0
L:	2.0	0.4	1.6	0.4	0.0	1.6	1.6	0.0	0.4	0.0	2.4	0.0	0.4	2.4	0.0	0.0	0.0	0.0	3.7	2.0	0.0	0.2	2.0	0.0	1.2	0.0
M:	2.4	0.4	0.4	0.2	0.0	0.0	2.0	0.0	0.4	0.0	4.1	2.4	0.0	0.1	0.0	0.0	0.0	2.4	2.4	2.0	0.0	0.0	0.0	0.0	0.2	0.0
N:	0.4	0.0	0.0	0.4	0.4	0.0	0.0	0.0	0.4	0.0	1.2	0.0	0.2	0.0	0.0	0.0	0.0	1.2	0.4	7.1	0.4	0.4	0.2	0.0	0.0	0.0
O:	0.0	0.1	0.4	2.0	9.3	2.8	1.2	0.8	0.1	0.0	0.0	1.6	0.0	1.2	0.0	0.4	0.0	3.2	0.4	6.9	0.0	0.0	0.0	0.0	0.0	0.0
P:	5.3	2.8	2.8	0.0	4.9	0.0	0.0	0.0	8.9	0.0	0.0	1.6	0.0	0.8	16.2	1.6	0.0	9.3	3.7	1.2	0.1	0.0	0.0	0.0	0.0	0.4
Q:	1.6	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
R:	4.3	0.0	2.0	1.6	0.0	1.6	2.7	0.0	0.0	0.0	0.4	2.4	2.0	2.0	0.0	1.2	0.0	0.4	0.1	2.7	0.0	0.4	0.0	0.0	0.0	0.0
S:	13.4	0.7	4.1	0.0	10.2	1.6	2.0	0.4	5.7	0.0	0.0	2.0	0.0	7.3	7.7	0.0	0.0	0.1	2.4	2.4	5.7	0.0	0.4	0.4	1.2	0.4
T:	21.9	0.1	2.0	0.4	83.6	0.0	0.0	0.0	15.8	0.0	1.2	0.2	2.8	0.8	8.5	2.0	0.0	6.1	0.8	0.1	1.2	0.0	0.8	0.8	2.0	0.0
U:	0.1	0.0	0.0	2.8	2.0	0.1	0.0	0.0	2.1	0.0	0.0	0.2	0.0	0.0	0.0	0.1	0.0	0.1	0.2	1.6	0.0	0.0	0.0	0.0	0.0	0.0
V:	0.0	0.0	0.0	0.4	2.4	0.0	1.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	4.1	1.2	1.2	0.0	0.0	0.4	0.0	0.0
W:	1.6	1.6	0.0	0.4	7.7	0.0	0.0	0.0	5.7	0.0	0.0	5.7	0.4	2.0	2.7	0.0	0.0	0.0	6.9	12.2	1.6	0.0	0.0	0.0	2.0	0.0
X:	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4	0.0	0.0
Y:	1.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	6.1	0.0	0.0	0.0	0.0	0.0
Z:	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4

	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:	4.1	0.0	1.1	23.5	7.3	1.2	2.4	0.0	0.4	0.0	0.8	2.8	1.2	0.8	7.7	4.5	0.8	1.2	2.8	6.1	1.2	0.4	0.4	0.0	2.4	0.0
B:	0.0	0.4	1.1	0.4	0.1	0.4	2.4	0.4	0.8	0.0	0.4	2.0	0.0	2.0	8.2	0.8	0.0	0.1	2.0	20.6	1.2	0.0	0.0	0.0	1.2	0.0
C:	6.9	0.0	0.0	0.0	2.0	0.4	0.0	0.0	0.2	0.0	0.0	2.0	12.2	17.6	4.5	1.2	0.0	4.1	7.2	1.6	0.7	0.0	0.0	0.0	0.4	0.0
D:	2.4	0.4	2.0	1.2	1.6	2.4	0.4	0.0	1.6	0.0	0.0	0.0	2.0	1.2	0.0	1.2	0.0	0.4	17.0	4.5	0.4	0.4	0.0	0.0	2.0	0.0
E:	2.0	0.0	2.0	0.4	7.3	0.8	1.2	0.0	4.1	1.2	0.0	0.0	0.4	0.0	3.2	6.9	0.0	1.2	2.4	4.1	0.4	0.0	0.0	0.0	0.0	0.0
F:	2.4	0.0	2.0	0.8	2.4	0.4	0.8	0.0	2.4	0.0	0.4	4.9	1.2	6.9	8.5	0.0	0.0	22.3	0.8	1.2	2.0	0.4	0.0	0.4	0.4	0.0
G:	2.0	0.4	0.0	0.0	0.0	0.0	0.4	0.0	1.6	0.0	0.0	0.0	0.0	0.0	2.7	0.0	0.0	2.0	0.0	2.0	0.0	2.0	0.0	0.0	0.0	0.4
H:	2.0	0.4	0.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	5.7	1.6	0.4	2.0	0.0	6.5	1.2	1.2	2.0	0.1	2.4	0.0	0.0	0.0
I:	2.0	0.0	2.0	1.2	1.2	2.4	0.0	0.4	1.6	0.0	0.0	0.0	0.4	0.4	0.0	4.5	0.0	0.4	4.9	6.5	0.0	0.2	0.0	0.0	0.0	0.0
J:	0.0	1.2	0.0	0.8	0.0	0.0	0.0	0.0	0.8	0.0	0.0	0.0	0.8	0.0	0.0	0.0	0.0	0.0	2.0	0.0	0.8	0.0	0.0	0.0	0.0	0.0
K:	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.2	0.8	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4	0.0
L:	2.0	0.4	1.6	0.4	0.0	1.6	1.6	0.0	0.4	0.0	2.4	0.0	0.4	2.4	0.0	0.0	0.0	0.0	3.7	2.0	0.0	0.2	2.0	0.0	1.2	0.0
M:	2.4	0.4	0.4	0.2	0.0	0.0	2.0	0.0	0.4	0.0	4.1	2.4	0.0	0.1	0.0	0.0	0.0	2.4	2.4	2.0	0.0	0.0	0.0	0.0	0.2	0.0
N:	0.4	0.0	0.0	0.4	0.4	0.0	0.0	0.0	0.4	0.0	1.2	0.0	0.2	0.0	0.0	0.0	0.0	1.2	0.4	7.1	0.4	0.4	0.2	0.0	0.0	0.0
O:	0.0	0.1	0.4	2.0	9.3	2.8	1.2	0.8	0.1	0.0	0.0	1.6	0.0	1.2	0.0	0.4	0.0	3.2	0.4	6.9	0.0	0.0	0.0	0.0	0.0	0.0
P:	5.3	2.8	2.8	0.0	4.9	0.0	0.0	0.0	8.9	0.0	0.0	1.6	0.0	0.8	16.2	1.6	0.0	9.3	3.7	1.2	0.1	0.0	0.0	0.0	0.0	0.4
Q:	1.6	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
R:	4.3	0.0	2.0	1.6	0.0	1.6	2.7	0.0	0.0	0.0	0.4	2.4	2.0	2.0	0.0	1.2	0.0	0.4	0.1	2.7	0.0	0.4	0.0	0.0	0.0	0.0
S:	13.4	0.7	4.1	0.0	10.2	1.6	2.0	0.4	5.7	0.0	0.0	2.0	0.0	7.3	7.7	0.0	0.0	0.1	2.4	2.4	5.7	0.0	0.4	0.4	1.2	0.4
T:	21.9	0.1	2.0	0.4	83.6	0.0	0.0	0.0	15.8	0.0	1.2	0.2	2.8	0.8	8.5	2.0	0.0	6.1	0.8	0.1	1.2	0.0	0.8	0.8	2.0	0.0
U:	0.1	0.0	0.0	2.8	2.0	0.1	0.0	0.0	2.1	0.0	0.0	0.2	0.0	0.0	0.0	0.1	0.0	0.1	0.2	1.6	0.0	0.0	0.0	0.0	0.0	0.0
V:	0.0	0.0	0.0	0.4	2.4	0.0	1.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	4.1	1.2	1.2	0.0	0.0	0.4	0.0	0.0
W:	1.6	1.6	0.0	0.4	7.7	0.0	0.0	0.0	5.7	0.0	0.0	5.7	0.4	2.0	2.7	0.0	0.0	0.0	6.9	12.2	1.6	0.0	0.0	0.0	2.0	0.0
X:	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4	0.0	0.0
Y:	1.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	6.1	0.0	0.0	0.0	0.0	0.0
Z:	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4

جدول رقم (6): العمود الثاني والثالث (10×10^{-2})

	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:	0.0	2.0	6.1	3.2	0.0	0.8	1.6	0.4	4.9	1.2	6.9	4.1	3.7	16.6	0.0	1.1	0.0	16.2	15.8	9.3	1.2	8.9	1.2	0.4	10.2	0.0
B:	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.1	0.0	0.0	2.1	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0
C:	1.2	0.0	2.0	0.0	0.4	0.0	0.0	0.4	1.2	0.0	0.4	0.0	0.0	0.0	1.2	0.0	0.4	0.4	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0
D:	1.2	0.0	0.0	1.6	1.2	0.0	0.0	0.0	2.0	0.0	0.0	0.0	0.4	0.0	0.4	0.0	0.4	0.0	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0
E:	20.5	2.0	9.7	1.6	9.2	4.1	2.9	0.0	0.2	0.4	0.0	9.7	5.3	6.1	2.3	3.0	0.0	15.4	13.2	11.4	0.4	1.6	2.0	0.8	0.4	0.0
F:	0.0	0.0	0.0	0.0	0.0	4.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0
G:	1.2	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
H:	25.6	0.0	0.0	0.0	93.0	0.0	0.0	0.0	19.9	0.0	0.0	0.0	0.0	0.0	16.2	0.0	0.0	4.1	0.4	0.0	0.0	0.0	0.0	0.0	1.2	0.0
I:	0.4	0.0	2.0	4.7	0.2	0.2	7.3	0.0	0.0	0.0	2.0	7.7	4.1	0.9	0.0	0.0	0.0	0.1	15.4	16.2	0.0	2.0	0.0	0.4	0.4	1.2
J:	0.0	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
K:	0.0	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
L:	6.5	0.0	0.0	1.2	1.6	0.0	2.1	0.0	1.2	0.0	0.0	3.2	0.8	0.0	0.1	0.0	0.0	0.0	2.2	1.6	1.2	0.0	0.1	0.0	0.0	0.0
M:	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.1	1.9	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
N:	1.6	0.0	2.0	25.0	4.1	3.2	0.0	0.4	3.7	1.2	0.0	2.0	0.0	1.2	2.0	0.0	0.0	0.4	2.4	0.7	0.0	3.2	0.0	0.0	2.4	0.0
O:	2.0	1.6	2.0	4.7	0.0	0.0	0.0	0.0	3.7	0.0	0.0	4.9	11.7	19.7	11.4	2.0	0.0	20.2	4.9	11.4	20.2	3.2	7.3	0.0	1.2	0.0
P:	3.4	0.0	0.0	0.0	5.8	0.0	0.0	0.0	0.8	0.0	0.0	0.4	0.0	0.0	1.0	1.5	0.0	0.4	0.2	0.4	0.0	0.0	0.0	0.0	0.0	0.0
Q:	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
R:	7.7	0.0	1.2	0.8	15.8	0.0	1.2	0.0	15.0	0.0	0.0	0.0	0.0	0.0	26.0	0.0	0.0	1.2	0.0	1.6	2.4	0.0	0.0	0.0	2.8	0.0
S:	0.0	0.4	0.4	0.0	2.0	0.0	0.0	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T:	6.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.6	0.0	0.0	0.0	0.0	0.0	3.2	0.0	0.0	3.7	1.2	0.4	3.7	0.0	0.0	0.0	0.0	0.0
U:	1.6	4.5	2.0	0.0	1.6	0.4	0.4	0.0	2.0	0.0	0.0	2.4	5.7	0.1	0.0	0.4	0.0	7.3	5.3	13.0	0.0	0.0	0.0	0.0	0.0	0.0
V:	0.1	0.0	0.0	0.0	9.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
W:	3.2	0.0	0.0	0.0	0.4	0.0	0.0	0.0	1.6	0.0	0.0	0.0	0.0	1.2	1.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
X:	0.0	0.0	0.4	0.0	0.1	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.7	0.0	0.0	0.0	1.6	0.0	0.0	0.0	0.0	0.0	0.0
Y:	0.4	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.4	1.2	0.0	1.6	0.0	0.0	2.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Z:	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4

جدول رقم (7): احتمالات حرف النص المشفر بالعمود الاول($10 x^{-2}$)

	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	0.0	0.0	0.0	0.0	10.5	0.0	1.6	5.3	12.9	0.0	0.0	7.9	2.6	1.6	0.0	4.0	0.0	0.0	4.0	7.9	0.0	0.0	0.0	0.0	1.6	0.0
B	7.7	3.8	0.0	1.9	0.0	0.0	0.0	3.8	38.5	0.0	1.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
C	20.8	5.2	9.1	0.0	2.6	0.0	2.6	0.0	5.2	2.6	2.6	5.2	0.0	5.2	10.3	1.3	1.3	6.5	0.0	2.6	6.5	1.3	1.3	0.0	3.9	0.0
D	8.9	0.0	8.9	11.2	0.0	1.3	0.0	5.1	3.8	0.0	3.8	8.9	5.1	0.0	16.5	7.6	0.0	10.1	1.3	0.0	0.0	3.8	3.8	0.0	0.0	0.0
E	4.1	0.0	4.1	4.1	19.7	0.0	0.0	0.0	13.1	0.0	0.0	9.8	6.7	11.5	0.0	9.4	0.0	3.3	4.9	2.5	0.0	0.0	1.6	0.0	3.3	0.0
F	7.5	1.9	1.9	11.5	15.9	3.8	0.0	0.0	0.0	0.0	0.0	1.9	9.4	11.3	5.7	0.0	0.0	9.4	3.8	9.4	1.9	0.0	0.0	0.0	4.7	0.0
G	1.6	1.6	3.9	0.0	17.2	6.3	2.4	0.0	1.6	0.0	0.0	0.0	0.0	27.6	12.5	1.6	0.0	5.4	6.3	3.1	0.0	0.0	0.0	0.0	0.0	0.0
H	6.3	0.9	1.8	0.0	8.1	0.9	0.9	11.7	0.0	0.0	0.0	0.0	8.1	0.9	0.9	27.9	6.3	0.0	0.0	8.1	5.9	3.6	0.0	0.9	0.0	0.0
I	9.2	2.0	1.0	3.1	18.2	3.1	2.0	4.1	14.3	0.0	0.0	0.0	0.0	1.0	3.1	1.0	10.2	0.0	9.2	1.0	12.2	6.1	2.0	1.0	0.0	0.0
J	1.0	1.0	1.5	1.0	21.5	0.0	2.5	5.1	9.2	0.0	0.0	0.0	0.0	0.0	3.1	2.7	1.0	0.0	21.5	1.0	0.0	5.0	2.7	0.0	0.0	0.0
K	5.0	0.0	2.5	4.9	5.9	2.5	3.9	4.1	10.0	2.0	1.0	0.0	0.0	0.0	11.0	0.0	0.0	25.5	12.2	0.0	0.0	1.0	0.0	1.0	1.0	0.0
L	6.3	0.0	0.0	4.7	9.4	0.0	2.4	2.4	7.1	0.0	0.0	7.9	0.0	0.0	0.0	5.5	0.0	3.1	22.0	22.0	3.9	0.0	1.6	0.0	0.0	0.0
M	7.7	0.9	0.9	0.0	10.9	4.5	0.0	0.0	8.0	1.8	0.0	3.6	3.6	0.9	1.8	0.0	0.0	2.7	1.8	8.9	7.1	0.0	1.0	0.0	0.7	0.0
N	3.4	3.4	1.1	0.0	3.4	7.9	0.0	4.7	11.2	1.1	1.1	4.5	2.8	13.7	0.0	0.0	0.0	10.7	0.0	1.1	12.4	2.2	0.0	0.0	1.1	0.0
O	7.4	4.9	11.1	1.2	0.0	0.0	2.5	3.7	3.7	1.2	1.2	3.7	6.2	7.4	17.3	0.0	0.0	0.0	16.0	2.5	1.2	3.7	1.9	0.0	0.0	0.0
P	6.4	1.1	4.6	3.7	12.1	0.0	0.0	1.1	11.4	0.0	0.0	2.3	5.8	1.2	11.0	6.4	0.0	0.1	0.0	11.0	2.3	0.0	1.7	0.0	0.0	0.0
Q	0.0	3.0	17.5	2.6	15.4	1.3	0.0	2.5	5.0	0.0	0.0	10.0	1.3	1.3	16.7	5.1	1.3	0.0	0.0	0.0	5.1	0.0	1.3	1.3	2.5	0.0
R	5.0	0.0	5.1	5.1	7.7	1.3	1.3	1.3	0.0	1.3	0.0	6.4	3.8	6.4	7.7	6.4	0.0	17.7	0.0	5.1	0.0	1.3	1.3	0.0	11.5	0.0
S	16.7	3.1	0.0	3.1	9.1	1.0	3.1	2.1	2.1	0.0	2.1	5.1	2.1	5.1	8.3	1.0	0.0	15.5	7.2	0.0	0.0	0.0	3.1	0.0	0.0	1.0
T	20.7	0.1	3.0	0.7	14.8	3.7	2.2	2.2	0.1	0.0	0.7	0.7	1.1	2.2	11.1	0.7	0.7	8.8	7.4	5.9	0.0	0.0	0.0	0.7	0.0	0.0
U	1.0	22.1	0.1	1.0	1.0	1.0	1.0	2.0	10.1	0.0	0.0	0.0	1.0	7.1	7.1	1.0	0.0	0.0	9.1	23.2	1.0	0.0	0.0	0.0	0.0	0.0
V	7.1	0.0	14.3	0.6	16.5	0.0	1.7	5.5	3.3	0.0	0.0	0.0	1.7	4.4	14.3	0.0	0.0	4.4	4.4	19.0	7.1	2.2	0.0	0.0	0.0	0.0
W	4.9	0.0	2.4	0.9	21.7	1.6	0.0	0.1	0.1	0.0	0.0	2.4	0.0	0.0	4.7	3.3	0.1	0.7	5.2	9.0	9.0	0.0	2.4	0.0	0.0	0.0
X	0.0	0.7	0.0	0.0	11	3.4	0.0	0.0	9.3	0.0	0.0	1.7	1.7	0.0	0.7	7.6	0.7	3.4	6.0	8.7	4.0	1.7	1.0	0.0	0.0	0.0
Y	1.2	0.0	9.8	2.4	4.9	12.2	6.1	1.2	1.2	1.2	2.4	6.1	6.1	1.6	1.2	1.2	1.2	12.2	1.2	13.4	3.7	0.0	2.4	2.4	1.2	0.0
Z	0.0	0.0	0.0	3.3	3.3	0.0	10.0	3.4	7.9	0.0	0.0	3.3	1.2	3.3	6.6	0.0	0.0	10.1	7.9	3.3	3.3	0.0	3.3	0.0	3.3	0.0

جدول رقم (8) : احتمالات النص المشفر للعمود الثاني($10 x^{-2}$)

	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	16.0	0.0	2.0	0.0	0.0	0.0	1.1	4.7	4.7	0.0	0.0	1.9	9.3	4.7	1.1	0.0	0.0	0.0	10.3	30.3	0.0	0.0	0.0	0.0	0.0	0.0
B	0.0	3.6	0.0	1.2	1.2	0.0	1.2	13.1	3.6	0.0	0.0	0.0	1.2	11.9	2.4	1.2	0.0	0.0	0.0	20.2	2.4	0.0	0.0	1.2	2.4	0.0
C	0.0	0.0	6.8	0.0	1.6	0.0	0.0	0.0	6.8	0.0	0.0	0.0	0.0	0.4	18.3	6.8	0.0	0.4	0.0	0.0	6.5	0.4	0.0	0.0	4.1	0.0
D	5.1	1.7	0.0	20.3	0.0	1.7	3.4	0.0	6.8	1.7	1.7	3.4	6.8	0.0	0.0	23.7	0.0	1.7	6.8	0.0	0.0	3.4	3.4	0.0	1.7	1.7
E	17.6	0.0	0.0	0.0	39.5	0.0	0.8	0.8	1.7	0.8	0.0	1.7	0.8	11.8	0.0	0.0	0.8	11.8	0.8	4.2	0.0	0.0	0.0	0.8	0.0	0.0
F	0.0	11.7	2.1	1.1	2.1	0.0	0.0	2.1	1.1	0.0	0.0	4.3	3.2	3.2	2.4	0.0	0.0	34.0	11.7	1.1	2.1	0.0	0.0	0.0	6.4	0.0
G	0.0	1.8	21.8	1.8	3.6	0.0	5.4	0.0	2.0	0.0	0.0	0.0	4.0	4.0	3.6	12.8	0.0	0.0	26.0	11.0	1.8	0.0	0.0	0.0	5.0	0.0
H	23.2	0.0	4.5	14.3	3.2	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	4.5	3.4	0.9	0.0	0.0	1.0	21.3	3.2	0.9	0.1	0.0	0.0	0.0
I	10.3	7.1	0.6	0.0	28.7	0.0	0.0	0.0	0.0	15.7	0.0	0.6	0.6	0.0	1.3	7.7	3.9	0.0	9.7	0.0	3.2	6.5	3.9	0.0	0.0	0.0
J	0.0	9.4	21.9	0.0	1.7	12.5	0.0	3.1	1.6	1.6	0.0	3.1	1.6	1.6	3.1	7.8	1.6	9.4	9.4	0.0	0.0	4.7	3.1	0.0	0.0	0.0
K	0.0	0.0	9.5	17.6	0.0	4.1	9.5	2.7	4.1	0.0	0.0	0.0	4.1	1.4	0.4	2.7	1.4	4.1	1.4	27.0	0.0	2.7	2.7	0.0	0.0	0.0
L	9.1	0.0	0.0	0.1	41.1	0.0	0.0	7.0	0.0	0.0	0.0	7.0	0.0	9.1	2.1	2.9	0.0	0.9	2.9	4.7	10.1	0.9	0.6	0.0	1.6	0.0
M	2.9	7.0	0.0	0.0	20.0	4.0	0.0	7.0	22.9	0.0	0.0	0.0	7.6	0.0	2.1	0.0	0.0	0.0	12.4	10.5	7.9	3.1	0.0	0.0	4.0	0.0
N	10.0	0.0	6.3	0.0	0.0	10.0	10.0	7.3	3.3	0.0	0.0	1.3	7.3	22.5	0.0	0.0	0.0	0.0	2.5	15.0	0.0	1.3	5.0	0.0	1.3	7.3
O	28.7	7.7	0.0	4.6	0.0	0.0	3.4	16.1	1.1	0.0	0.0	3.4	0.0	1.1	0.0	27.5	0.0	0.0	0.0	0.0	4.6	7.7	0.0	1.1	0.0	0.0
P	0.9	7.4	8.3	0.9	3.6	0.0	0.0	5.3	31.0	0.0	0.9	16.7	0.5	1.9	1.5	1.6	0.0	0.0	0.9	1.9	0.9	1.9	1.5	0.0	1.9	0.0
Q	0.0	0.0	18.9	9.0	1.1	2.7	0.0	0.0	29.7	1.4	0.0	1.4	14.5	1.4	1.1	0.0	0.0	0.0	2.7	5.1	1.4	0.0	2.1	1.4	0.0	0.0
R	0.1	0.0	3.0	10.1	10.2	0.0	0.0	0.0	0.0	2.0	3.0	0.0	0.0	33.3	1.0	0.0	0.0	24.2	0.0	3.0	2.0	0.0	0.0	1.0	0.0	0.0
S	3.3	3.6	0.0	0.0	30.3	3.6	0.0	1.0	0.0	0.0	0.0	11.1	0.0	3.6	20.2	0.0	0.0	0.0	11.0	0.0	0.0	0.0	1.0	0.0	1.0	0.0
T	4.9	0.0	4.9	0.0	0.0	0.0	0.0	2.5	0.0	0.0	0.0	0.0	0.0	13.6	0.0	4.1	17.1	0.0	0.0	20.5	0.0	0.0	0.0	0.0	0.0	7.2
U	0.1	0.2	1.1	4.7	1.1	1.1	13.6	4.8	3.4	0.0	0.0	0.0	0.0	10.2	33.0	0.0	1.1	1.1	1.1	0.2	0.0	6.8	0.2	0.0	1.1	0.0
V	1.4	0.7	0.7	2.1	17.6	0.0	1.4	18.3	6.3	0.7	0.7	0.0	0.0	7.7	20.4	0.0	0.7	19.7	0.0	0.0	0.0	0.0	0.0	0.7	0.7	0.0
W	1.7	0.0	4.1	0.0	3.0	10.7	0.0	0.8	28.1	0.8	0.8	5.3	0.0	0.8	10.7	0.6	0.0	2.3	12.7	0.8	0.0	0.0	5.6	1.0	0.8	0.0
X	2.5	0.0	0.0	6.3	0.4	0.0	0.0	0.0	5.7	1.3	2.5	0.0	0.0	3.8	0.0	0.0	1.3	1.3	2.5	44.3	1.3	1.3	1.3	0.0	0.0	0.0
Y	5.3	0.0	0.0	1.1	14.0	4.2	2.7	12.6	0.0	0.0	1.1	4.2	7.1	6.3	0.0	0.0	0.0	21.1	0.0	3.2	15.8	0.0	0.0	0.0	5.3	0.0
Z	0.0	0.0	0.0	0.0	3.0	1.0	3.0	0.0	10.4	0.0	0.0	16.0	3.0	0.0	0.0	0.0	0.0	19.0	27.4	0.0	3.0	0.0	0.1	0.0	0.0	0.0

جدول (9): احتمالات النص المشفر بالعمود الثالث($10 x^{-2}$)

	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	21.1	0.0	3.2	0.0	2.1	0.0	0.0	9.5	10.7	1.1	0.0	3.2	1.1	0.4	9.5	3.2	0.0	0.0	7.4	2.1	4.2	0.0	7.4	0.0	3.2	0.0
B	1.3	6.6	0.0	2.6	0.0	2.6	2.6	2.6	17.1	1.3	2.6	0.0	6.6	18.4	11.8	2.6	1.3	1.3	0.0	17.1	0.0	0.0	0.0	0.0	1.3	0.0
C	7.7	1.3	6.4	0.0	5.1	0.0	2.6	0.0	5.1	1.3	0.0	15.4	0.0	7.7	11.5	3.8	0.0	0.0	2.6	0.0	6.4	0.0	0.0	0.0	7.7	1.3
D	6.4	2.1	2.1	6.4	2.1	2.1	0.0	0.0	4.3	2.1	0.0	12.8	10.6	2.1	6.4	12.8	0.0	0.0	6.4	6.4	2.1	0.0	0.0	0.0	4.3	0.0
E	20.5	0.0	6.8	0.0	21.6	1.0	0.0	0.0	3.5	0.0	1.0	5.5	1.0	8.8	1.0	2.0	2.0	5.8	3.5	3.5	0.0	0.0	2.5	0.0	1.0	1.0
F	1.1	0.4	3.2	6.2	6.3	6.2	0.0	2.1	0.0	0.0	0.0	0.0	3.2	5.3	6.2	21.1	0.0	0.0	16.7	10.5	0.4	1.1	1.1	0.0	0.0	0.0
G	3.2	0.0	10.5	0.0	5.6	0.0	2.4	0.0	0.2	0.0	0.0	0.0	2.4	2.4	12.1	12.9	4.0	0.0	3.2	10.7	10.5	0.0	0.0	0.0	0.0	1.6
H	0.0	2.0	1.0	6.1	14.1	1.0	0.0	14.1	0.0	0.0	0.0	1.0	1.0	6.1	15.2	11.1	1.0	1.0	6.1	15.2	2.0	1.0	1.0	0.0	0.0	0.0
I	21.9	0.0	2.6	2.6	31.7	1.6	0.8	0.8	8.7	0.0	0.0	0.0	0.8	9.2	4.0	6.2	0.0	12.7	0.0	0.8	7.1	0.8	0.0	0.0	0.0	0.0
J	1.5	4.5	0.0	3.0	4.5	13.4	0.0	0.0	1.5	1.5	0.0	4.5	0.0	1.5	13.4	0.0	1.5	13.4	20.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
K	2.2	1.1	5.6	0.0	8.9	1.1	10.0	3.3	7.8	0.0	1.1	1.1	1.1	1.1	4.4	1.1	0.0	20.0	3.3	15.6	0.0	1.1	3.3	2.2	4.4	0.0
L	10.1	0.0	1.0	7.1	0.0	1.0	1.0	14.1	10.1	0.0	0.0	8.1	0.0	0.0	0.0	6.1	0.0	6.1	13.1	13.1	8.1	0.0	0.0	0.0	1.0	0.0
M	4.3	2.6	0.9	0.0	18.1	0.0	1.7	1.7	26.7	0.0	0.9	1.7	6.0	0.0	2.6	0.0	0.0	5.2	6.0	11.2	1.6	0.9	0.0	0.0	0.9	0.0
N	17.2	3.1	3.1	1.6	1.6	6.3	0.0	0.0	6.3	4.7	0.0	1.6	3.1	17.2	0.0	0.0	0.0	3.1	1.6	10.9	10.9	3.1	3.1	0.0	1.6	0.0
O	6.3	6.3	6.3	2.5	2.5	0.0	6.3	0.0	1.3	1.3	3.8	6.3	7.5	3.8	23.8	0.0	0.0	0.0	1.3	6.3	3.8	2.5	2.5	1.3	0.0	0.0
P	6.0	4.0	6.0	6.0	18.1	2.4	0.0	6.0	3.6	0.0	0.0	12.0	6.0	7.2	2.4	7.2	0.0	4.0	0.0	1.2	1.2	0.0	1.2	1.2	2.4	0.0
Q	1.4	2.8	9.7	5.6	20.8	4.2	0.0	1.4	12.5	0.0	0.0	1.4	11.1	2.8	5.6	0.0	0.0	0.0	5.6	2.8	1.4	2.8	1.4	0.0	6.9	0.0
R	8.3	0.0	2.8	9.3	15.7	3.7	3.7	1.9	0.0	0.0	0.0	0.9	0.9	20.4	3.7	0.0	0.0	20.4	0.0	4.6	0.0	0.9	0.0	0.9	1.9	0.0
S	10.1	3.4	0.0	0.0	20.1	2.2	2.2	3.4	2.2	0.0	1.1	0.0	2.2	3.4	21.5	1.1	0.0	0.0	6.7	0.0	1.1	0.0	0.0	0.0	1.1	0.0
T	10.4	0.0	0.0	0.0	0.0	0.0	0.0	4.3	7.0	0.0	0.0	0.0	0.1	0.0	4.3	5.2	14.0	0.0	5.2	0.0	17.1	0.0	0.0	0.0	0.0	0.0
U	3.1	1.5	6.2	12.3	0.0	4.6	4.6	9.2	20.0	0.0	0.0	0.0	0.0	3.1	1.5	3.1	0.0	0.0	9.2	6.2	3.1	10.8	0.0	0.0	0.0	1.5
V	0.0	2.7	10.8	0.1	10.1	0.0	0.0	4.5	12.7	0.0	0.0	0.0	0.0	0.0	4.5	0.0	1.8	0.0	21.8	3.6	4.5	0.0	0.0	0.0	0.0	0.0
W	0.0	0.0	4.7	4.7	17.0	7.5	0.0	2.0	13.1	1.0	0.0	0.0	0.0	0.0	10.0	0.0	0.0	1.0	22.4	1.0	2.0	0.0	0.0	0.0	0.0	0.0
X	0.0	0.0	1.0	0.0	27.5	0.0	2.9	1.0	1.0	0.0	1.0	1.0	3.9	2.9	0.0	7.8	0.0	1.0	3.9	34.3	0.0	0.0	1.0	0.0	0.0	0.0
Y	5.1	0.0	0.0	0.0	11.4	5.1	0.0	10.1	2.5	0.0	1.3	7.6	6.3	2.5	3.8	0.0	1.3	0.0	1.3	0.0	14.5	1.3	0.0	0.0	2.5	0.0
Z	0.0	2.0	1.0	0.0	0.1	6.1	2.0	13.1	10.2	0.0	2.0	7.1	3.0	0.1	0.1	0.0	0.0	0.1	0.0	0.1	0.0	2.0	0.0	0.0	1.0	1.0

جدول (10) : عدد ونسب احتمالاتها لحروف النص المشفر حسب الاعمدة

الحرف المشفر	عمود المفتاح المستحدم	عدد الحروف الصريحة	مجموع احتمالياتها %	عدد الحروف الصريحة التي لم تظهر
A	الاول	10	90,3	7
	الثاني	14	100	12
	الثالث	14	97,9	10
B	الاول	14	96,7	9
	الثاني	8	92,86	12
	الثالث	12	93,42	9
C	الاول	15	94,81	7
	الثاني	11	100	15
	الثالث	14	94,87	8
D	الاول	15	100	11
	الثاني	11	88,14	8
	الثالث	18	100	8
E	الاول	13	92,62	5
	الثاني	6	90,67	11
	الثالث	12	94,12	8
F	الاول	15	100	11
	الثاني	11	94,86	10
	الثالث	13	95,8	9
G	الاول	9	89	7
	الثاني	15	100	11
	الثالث	13	94,35	7
H	الاول	12	93,6	9
	الثاني	9	94،64	12
	الثالث	10	91,92	8
I	الاول	12	92,31	8
	الثاني	10	96,77	12
	الثالث	11	95,24	10
J	الاول	15	96,9	8
	الثاني	12	92,17	9
	الثالث	12	92،54	9
K	الاول	10	94,6	10
	الثاني	13	95,95	10
	الثالث	13	91,11	5
L	الاول	14	94,6	7
	الثاني	12	96,9	11
	الثالث	10	96	12
M	الاول	15	96,3	7
	الثاني	13	100	13
	الثالث	10	91,38	9
N	الاول	13	96,1	9
	الثاني	11	92,5	9

	الثالث	13	92,19	8
O	الاول	14	100	12
	الثاني	12	100	14
	الثالث	15	95	7
P	الاول	14	97،27	9
	الثاني	13	94,44	7
	الثالث	15	95,18	7
Q	الاول	13	94،38	8
	الثاني	9	91,9	11
	الثالث	13	93,06	8
R	الاول	14	96،06	8
	الثاني	12	100	14
	الثالث	12	96,3	10
S	الاول	15	95,41	6
	الثاني	8	92,86	10
	الثالث	11	95,51	11
T	الاول	14	95،56	6
	الثاني	13	100	13
	الثالث	11	95،65	10
U	الاول	14	95،96	8
	الثاني	10	92,05	9
	الثالث	11	95,45	10
V	الاول	11	95،6	11
	الثاني	7	92,25	10
	الثالث	11	95,45	10
W	الاول	14	96,75	9
	الثاني	10	93,39	9
	الثالث	13	95,33	8
X	الاول	10	92,37	10
	الثاني	10	91,14	9
	الثالث	9	93،14	10
Y	الاول	14	89,02	3
	الثاني	14	100	12
	الثالث	13	94,94	9
Z	الاول	15	100	11
	الثاني	10	93,4	9
	الثالث	14	97	9

المصادر

[1] William Stallings ," Cryptography and Network Security Principles and Practices, Prentice Hall, 2011.

[2] Alan G. Konhem ,Computer Security and Cryptography, John Wiley & Sons, Inc., Hoboken, New Jersey, 2007.

[3] Vikram Jain, A Code-Book Cipher Methodology for wireless Networks, IJCST Vol. 2, Iss ue 1,India, March 2010.

[4] R.F. Curchhouse , codes and ciphers, Cambridge university 2002 .

[5] Letter frequency, From Wikipedia, the free encyclopedia, 2007.

[6] Janeczko, Paul. Top Secret: A Handbook of Codes, Ciphers, and Secret Writing. Broadway, New York: Scholastic Inc., 2004.

[7] Dejan Ristanovic and Jelica Protic, "the book cipher algorithm", Dr Dobbs journal,2008.

[8] Natarajan Meghanathan, Classical Ciphers and their Cryptanalysis, Jackson State University, 2004.

Weak points in book cipher system

Qasim Mohammed Hussein
Tikrit University

(Received: 17 / 2 / 2013 ---- Accepted: 17 / 3 / 2013)

Abstract

This paper includes determining the weak points of cryptosystem that use the letters of a certain book as key in encryption and decryption processes. It depends on study the letters frequency distribution of cipher text and the characteristics of the language that is used in writing the book rather than the language of the plain text. It takes in consideration, using English language in writing the plain text, key, and cipher text. The research finds much vulnerability that can be explored to reduce the key space and reduce the number of possibilities when attack the encrypted message in this system. For example, there is ability to reduce the possibility number of key letter of for the first three columns from 17576 to 2475 with percentage 90.9%. And the relation between columns letters reduced between 50% and 73%. Besides, the possibilities of the plain letters for each cipher text letter can reduced with 50%.