

المحاضرة السابعة

# التعويض متعدد الحروف الهجائية

# التعويض متعدد الحروف الهجائية

- إن نظام التشفير الذي يستخدم هجائيتين أو أكثر في عملية التعويض يدعي النظام التعويضي المضاعف أو متعدد الحروف الهجائية
- الهجائيات المضاعفة مثل الشفرات القيصرية والهجائيات العشرية
- من هذه الهجائيات جدول فاجر وسميت بذلك الاسم نسبة لمحلل الشفرة الفرنسي والذي يعتبر أول من استخدمها

# التعويض متعدد الحروف الهجائية

- الجدول الأتي يمثل جدول فنجر ولغرض القيام بعمليات التشفير يمثل سطر الحروف العلوي في الجدول النص الصريح
- يمثل العمود الأيسر في الجدول أحرف المفتاح

# جدول فنجر

- 0 A ABCDEFGHIJKLMNOPQRSTUVWXYZ •
- 1 B BCDEFGHIJKLMNOPQRSTUVWXYZA •
- 2 C CDEFGHIJKLMNOPQRSTUVWXYZAB •
- 3 D DEFGHIJKLMNOPQRSTUVWXYZABC •
- 4 E EFGHIJKLMNOPQRSTUVWXYZABCD •
- 5 F FGHIJKLMNOPQRSTUVWXYZABCDE •
- 6 G GHIJKLMNOPQRSTUVWXYZABCDEF •
- 7 H HIJKLMNOPQRSTUVWXYZABCDEFG •
- 8 I IJKLMNOPQRSTUVWXYZABCDEFGH •
- 9 J JKLMNOPQRSTUVWXYZABCDEFGHI •
- 10 K KLMNOPQRSTUVWXYZABCDEFGHIJ •
- 11 L LMNOPQRSTUVWXYZABCDEFGHIJK •
- 12 M MNOPQRSTUVWXYZABCDEFGHIJKL •
- 13 N NOPQRSTUVWXYZABCDEFGHIJKLM •
- 14 O OPQRSTUVWXYZABCDEFGHIJKLMN •
- 15 P PQRSTUVWXYZABCDEFGHIJKLMNO •
- 16 Q QRSTUVWXYZABCDEFGHIJKLMNOP •
- 17 R RSTUVWXYZABCDEFGHIJKLMNOPQ •
- 18 S STUVWXYZABCDEFGHIJKLMNOPQR •
- 19 T TUVWXYZABCDEFGHIJKLMNOPQRS •
- 20 U UVWXYZABCDEFGHIJKLMNOPQRST •
- 21 V VWXYZABCDEFGHIJKLMNOPQRSTU •
- 22 W WXYZABCDEFGHIJKLMNOPQRSTUV •
- 23 X XYZABCDEFGHIJKLMNOPQRSTUVW •
- 24 Y YZABCDEFGHIJKLMNOPQRSTUVWX •
- 25 Z ZABCDEFGHIJKLMNOPQRSTUVWXY •

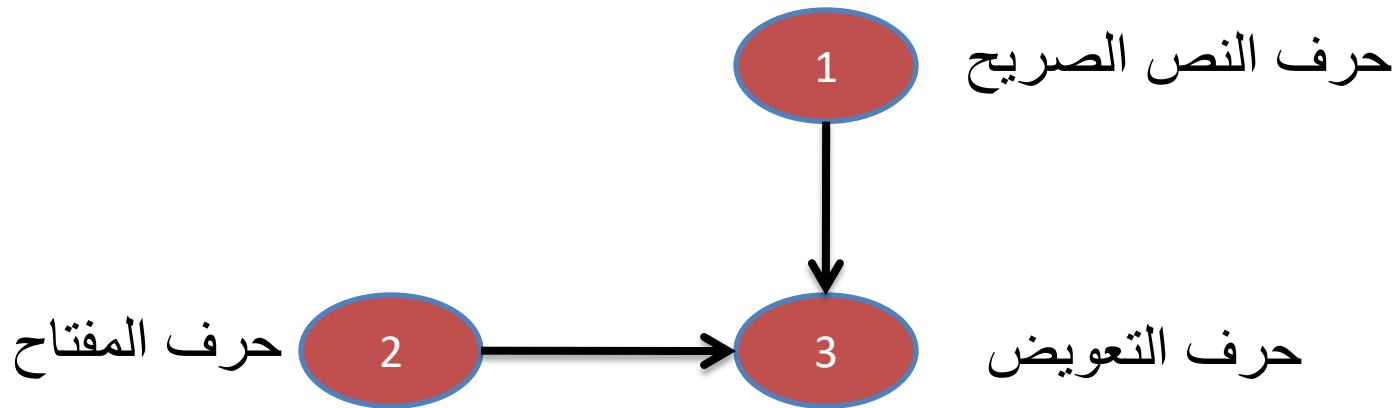
د عثمان محمد دفع الله  
أستاذ مشارك جامعة كرري

# التشفير باستخدام جدول فنجر

- أفرض أن النص الصريح المطلوب تشفيره هو  
CARRY OUT PLANS B WEDNESDAY  
END في هذه الحالة تكرر كلمة المفتاح تحت النص الصريح  
ويتم تعويض الحروف من الهجائية المشار اليها سابق  
■ بالنسبة للمثال الحالي يصبح لدينا ما يلي  
CARRY OUT PLAN B WEDNESDAY  
ENDEN END ENDE N DENDENDE  
GNUVL RYG SPNQ F JHHAHWQDC

# التشفير باستخدام جدول فنجر

- كل حرف تعويضي يمكن إيجاده بالاتجاه نحو أسفل العمود الذي يحتوي حرف النص الصريح حتى الوصول إلي حرف المفتاح



# التشفير باستخدام جدول فنجر

- هنالك طريقة أبسط لاستخدام جدول فنجر وذلك بكتابة كلمة المفتاح أولاً مع وضع النص الصريح بعد ابداله بحيث يكون مجاوراً لها
- مثلاً لنفس الرسالة السابقة

المفتاح

النص الصريح

E

C R U L B D S Y

N

A Y T A W N D

D

R O P N E E A

# التشفير باستخدام جدول فنجر

النص المشفر      المفتاح

E    G V Y P F H W C

N    N L G W J A Q

D    U R S Q H H D

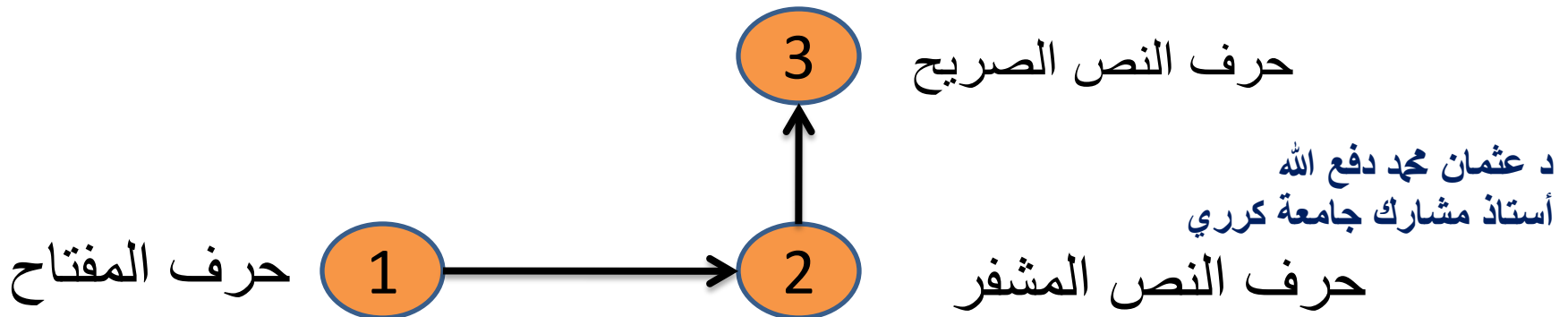
ليصبح النص المشفر

GUN VLR YGS PNQ JFH HAH WQDC



# التشفير باستخدام جدول فنجر

- لغرض حل شفرة التعويضات المتعددة الهجائيات يجب أن يكون المستلم علي علم بالمفتاح ويجب كذلك أن يعلم بالنص المشفر
- يتم الدخول إلي جدول فنجر من جانب حرف المفتاح حيث نجد الحرف المشفر ثم نأخذ اتجاه الصعود إلي اعلي الجدول لإيجاد حرف النص الصريح كما يوضح الشكل التالي



# التشفير باستخدام جدول فنجر

■ إذا كانت لدينا الرسالة المشفرة الآتية

TUAEIGTUEISBLNCCUAS

إذا كان المفتاح هو RUN أوجد النص الصريح

R	T	E	T	I	L	C	S		C	N	C	R	U	L	B
U	U	I	U	S	N	U		النص الصريح	A	O	A	Y	T	A	
N	A	G	E	B	C	A	→		N	T	R	O	P	N	

تظهر الرسالة الصريحة كالآتي

CAN NOT CARRY OUT PLAN B

# التعويض التخطيطي

- في التعويض التخطيطي يتم تجزئيه النص الصريح إلى أزواج من الحروف ويتم إبدال كل زوج من النص الصريح بزواج تعويضي من النص المشفر
- من أشهر أنظمة التشفير التخطيطي شفرة بليفر
- هذه الشفرة تستخدم مربعا أبعاده (5X5) تحتوي علي الأحرف الهجائية
- توضع الهجائية في مثل هذا المربع باتجاه عقارب الساعة كما يأتي

# التعويض التخطيطي

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 •

• في هذا المربع تم حذف حرف ال Z

# التعويض التخطيطي

• قواعد التشفير تأخذ الأشكال الآتية :-

I. إذا كان الحرفان للزوج في نفس الصف تكون مكافئتهما للنص المشفر هما الحرفان الواقعان بينهما مباشرة مثال علي ذلك

AC → BD

II. إذا كان حرف النص الصريح في آخر الصف نقوم بتعويض الحرف الموجود في النهاية المعاكسة لنفس الصف مثال علي

ذلك ST → TP و KO → LK

III. إذا كان الحرفان في نفس العمود فتكون مكافئتهما للنص المشفر هما الحرفان الواقعان مباشرة تحت كل منهما مثال علي ذلك

# التعويض التخطيطي

IX → EY و YE → EJ •

IV. إذا كان الحرفان في الزاويتين المتقابلتين لمستطيل وهمي متعاكستين قطريا فتكون مكافئتهما هما الحرفان في القطر المعاكس نبدأ عملية التعويض بأول حرف من النص الصريح ويعوض حرف النص المشفر في نفس الصف مثال علي ذلك

EK → AO

SE → TD

# التعويض التخطيطي

- تحتاج عملية فك الشفرة للنص المشفر بطريقة بليفر أن المستلم يعلم بمحتويات المربع ذي الأبعاد (5X5) إضافة الي قواعد التشفير لغرض عكس الرسالة
- لتحويل مربع بليفر يستخدم مفتاح معين ويكون المربع هو (5X5) بنفس الطريقة مثال علي ذلك اذا كانت كلمة المفتاح هي CODE فيكون مربع بليفر كالآتي
- CODEA
- BFGHI
- JKLMN
- PQRST
- UVWXY