**المحاضرة التاسعة:**

**ملاحظة:** جميع الطرائق التعويضية التي سبق شرحها تسمى (Mono. alphabetic cipher والتي تقع كفرع اساسي للطرائق القديمة.

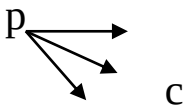
## Homophonic substitution ciphers

في هذه الطرق كل حرف في النص الصريح Plain text يقابل اكثر من رقم في الـ Cipher text

(mopping - is - one - to – many)

**Note:** Each plain text character encrypted with a variety of cipher text character.

Substitutes




P: help

C :23...

Number of substitution are being proportional to the frequency of letters.

# Example:

| plain | Cipher |
|---|---|
| A | 9 12 33 47 53 67 78 92 |
| B | 86 82 81 98 |
| C | 13 41 62 |
| D | 01 03 45 79 |
| E | 14 16 24 44 46 55 57 |
| F | 10 13 |
| G | 6 25 |
| H | 23 39 50 56 65 68 |
| I | 32 10 73 83 88 93 |
| J | 15 64 74 |
| K | 4 71 91 |
| L | 26 37 51 84 |
| M | 22 27 |
| N | 18 85 58 59 66 |
| O | 5 7 54 72 90 99 |
| P | 38 95 |
| Q | 44 22 |
| R | 29 35 40 52 77 |
| S | 11 19 36 76 86 |
| T | 17 20 30 43 49 |
| U | 8 61 63 |
| V | 34 75 85 91 |
| W | 60 89 |
| X | 28 69 |
| Y | 21 52 |
| Z | 0 2 80 |

**ملاحظة:** هذا الجدول غير ثابت يعني يمكن أن يتغير.

في الجدول اعطينا معوضات Substitution للحروف الأبجدية. هنا تكون عبارة عن ارقام من (0….99) بمعنى كل حرف يعطي مجموعة من الأرقام حسب تكراره (وروده في بارات)

**Example:** Encrypt the plain text [Mosul University] using homophonic substitution

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P : | m | o | s | u | l | v | n | i | v | e | r | s | i | t | y | |
| C : | 22 | 5 | 11 | 8 | 26 | 81 | 18 | 32 | 34 | 14 | 23 | 11 | 10 | 17 | 21 | |

**Beale Cipher:** تم اكتشاف هذه الطريقة من قبل الباحث Beale وتتضمن الخطوات التالية

1. نكون نص افتراضي يحتوي على جميع الاحرف المكتوب بها النص الأصلي
2. ناخذ احرف النص الافتراضي ونثبتها بجدول بدون تكرار وامام كل حرف نضع عدة ارقام افتراضية او مختلفة او عشوائية.
3. ناخذ كل حرف من النص الأصلي ونضع امامه مايقابل الحرف في الجدول واذا تكرر الحرف ناخذ الرقم الثاني وهكذا …..

**مثال:**

شفر كلمة computer باستخدام شفرة Beale؟

**أولا:** نفرض النص الافتراضي:

Text : come here and put the letter

**ثانيا:** نشكل الجدول كالآتي:

| plain | cipher |
|---|---|
| c | 1 30 |
| o | 5 17 |
| m | 12 80 |
| e | 9 3 13 24 22 |
| h | 27 26 |
| r | 78 18 |
| a | 11 56 |
| n | 55 77 |
| d | 7 21 |
| p | 32 39 |
| u | 19 44 |
| t | 25 14 34 |
| l | 75 15 |

plain text : computer

c o m p u t e r

1 5 12 32 19 25 9 78

Cipher text: 1512321925978

**توضيح:** هذه الفكرة أتت انه كلما كانت الحروف المقابلة للنص متنوعة تكون أفضل اي كل حرف نعطيه أكثر من معوض كي نعيق عملية التحليل أمام المحلل حتى لا يستفاد من سبب تكرار الحروف.