التشفير : هو عملية تحويل المعلومات من نص بسيط ومفهوم الى نص غير مقروء للحفاظ على خصوصية الفرد وأمان المعلومات.

أنواع التشفير : ينقسم التشفير إلى نوعين تشفير متماثل وتشفير غير متماثل:

التشفير المتماثل يعتمد على مفتاح واحد لتشفير النص وفك شفرته، أما **التشفير غير المتماثل** فيعتمد على مفتاحين أحداهما لتشفير النص والأخر لفك شفرته.

تطبيق للتشفير: مثلا شفر كلمة **الحاسب** بالاعتماد على مفتاح **التشفير k=5**

الحرف الأصلي	أ	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ك	ل	م	ن	ه	و	ي
الحرف بعد التشفير	ح	خ	د	ذ	ر	ز	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ك	ل	م	ن	ه	و	ي	أ	ب	ت	ث	ج

أ ⟸ ح

ل ⟸ ي

ح ⟸ ز

أ ⟸ ح

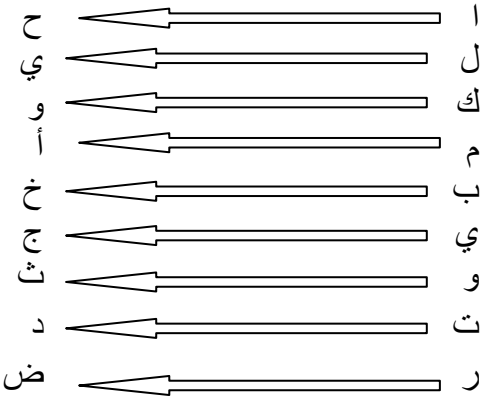
س ⟸ ظ

ب ⟸ خ

فكلمة الحاسب بعد التشفير تصبح : حيزحظخ

لو أردنا إعادة فك التشفير نستخدم نفس الجدول مثال حرف ح (الحاء) بعد عملية التشفير ينتج لنا حرف الألف وهنا نفس المفتاح في عملية التشفير وعملية فك التشفير.

مثال 2: شفر كلمة الكمبيوتر بالاعتماد على مفتاح التشفير k=5



حيوأخجثدض هي الكلمة المشفرة ل: الكمبيوتر

شفرة القيصر : وهي من أقدم أنواع التشفير باستخدام تقنيات تبديل الحروف ، ويتم استبدال الحرف بالحرف الثالث الذي يليه ـأو الحرف بالرقم .

مثال تطبيقي مثلا: هذه أحرف من A إلى Zمبدلة بالمفتاح رقم 3(K=3) أي كل حرف يتبدل بالحرف الثالث الذي ليه يعني:A أصبح D.....الخ

والمثال التالي يوضح :

هذه ترتيب الأحرف باللغة الأجنبية:

A – B – C- D- E- F- G- H- I- J- K- L – M –N –O -P- Q- R -S -T -Y- V-W- X- Y –Z

بعد عملية التشفير وبالاعتماد على مفتاح التشفير K=3 تصبح كالتالي:

D - E- F- G –H –I – J- K –L –M –N –O –P –Q -R-S-T-U-V-W-X-Y-Z-A-B-C

كما تعتمد شفرة القيصر على معادلة :X=m+K(mod26)

Xهو النص المشفر

Kهو مفتاح التشفير

mod 26 وهي: system modules والرقم 26 هو عدد أحرف اللغة الانجليزية

مثال: لدينا كلمة root security ونريد تشفيرها ضمن قيمة المفتاح k=4

$^{0}A – ^{1}B – ^{2}C- ^{3}D- ^{4}E- ^{5}F- ^{6}G- ^{7}H-^{8} I- ^{9}J-^{10} K- ^{11}L – ^{12}M –^{13}N –^{14}O -^{15}P- ^{16}Q- ^{17}R -^{18}S - ^{19}T ^{-20}Y-^{21} V-^{22}W- ^{23}X-^{24} Y –^{25}Z$

C=(r+4)mod26=(17+4)mod26=21=v

C=(o+4)mod26=(14+4)mod26=18=s

C=(o+4)mod26=(14+4)mod26=18=s

C=(t+4)mod26=(19+4)mod26=23=x

وبالتالي تصبح كلمة root بعد تشفيرها تعني : vssx

Security :

C=(s+4)mod26=(18+4)mod26= 22 =w
C=(e +4)mod26=(4 +4)mod26=8 =i
C=(c +4)mod26=(2 +4)mod26=6 =g
C=(u +4)mod26=(20+4)mod26=24 =y
C=(r+4)mod26=(17+4)mod26= 21 =v
C=(i +4)mod26=(8 +4)mod26= 12 =m
C=(t +4)mod26=(19+4)mod26= 23 =x
C=(y +4)mod26=(24+4)mod26= 2 =c
28-26=2**(يتم طرح العدد**
الأكثر من 26 وهو الموضح في جمع24+4=28 وهنا نطرح 28-26 =2)

ومنه فكلمة securityبعد تشفيرها تصبح: wigyvmxc

تطبيق 3: وفق شفرة قيصر وبمفتاح k=3شفرة الكلمة التالية: technologie

A – B – C- D- E- F- G- H- I- J- K- L – M –N –O -P- Q- R -S -T -Y- V-W- X- Y –Z
نأخذ الكلمة ونفكك كل حرف على حدا وما يقابله برقم ثالث يليه (وهنا كوننا نعتمد على المفتاحk=3)

T ⟶ w
E ⟶ h
C ⟶ f
H ⟶ k
N ⟶ q
O ⟶ r
L ⟶ o
O ⟶ r
G ⟶ j
I ⟶ L
e ⟶ h

ومنه فكلمة technologie بعد تشفيرها تصبح: whfkqrorjlh