

نأخذ مثال شامل للتشفير وفك التشفير بهذه الطريقة :

لدينا النص التالي : **THE PROFESSOR IS EVIL** ونريد تشفيره من البروفيسور ☺ .

الآن أولاً نختار النوع الذي نريد نم شفره hill هل هو 2 ، أو 3 أو 4 .

ونختار 2-Hill Cipher ، لأنه النوع الأسهل .

الآن نقوم في البداية بتقسيم النص الأصلي إلى مجموعات Block كل واحد منها مكون من حرفين (لأننا اخترنا 2-Hill Cipher ، في حاله اخترنا n سوف تقسم الحروف في النص الأصلي إلى n حرف) .

(لاحظ أننا سنعتمد هنا أن الحرف الأول A تكون قيمته 1 وليس 0 ، كما كنا نشفر في الشفرات السابقة ، طبعاً يمكنك أتباع الأسلوب القديم وهو الحرف A تكون قيمته 0) .

T	H	E	P	R	O	F	E	S	S	O	R	I	S	E	V	I	L
20	8	5	16	18	15	6	5	19	19	15	18	9	19	5	22	9	12

ونقوم الآن بوضع هذه الأرقام في مصفوفة النص الأصلي P .

$$P = \begin{pmatrix} 20 & 5 & 18 & 6 & 19 & 15 & 9 & 5 & 9 \\ 8 & 16 & 15 & 5 & 19 & 18 & 19 & 22 & 12 \end{pmatrix}$$

الآن نختار مصفوفة التشفير والتي يجب أن يكون لها معكوس حتى نستطيع فك التشفير .

$$A = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$$

(يمكنك التأكد من ذلك ، وذلك عن طريق أخذ det وضربه في عدد ما (المعكوس) واخذ الناتج mod 26 ويجب أن يكون الباقي يساوي 1 ، وهنا نتأكد من أن المصفوفة صحيحة ولها معكوس) .

الآن نقوم بضرب المصفوفة p في المصفوفة A لكي ينتج لدينا المصفوفة c (الشفره)