$$E = AP = \begin{pmatrix} 148 & 121 & 180 & 60 & 209 & 183 & 159 & 157 & 117 \\ 64 & 58 & 81 & 27 & 95 & 84 & 75 & 76 & 54 \end{pmatrix}$$

الآن نأخذ الناتج 26 mod (لجميع القيم في المصفوفة بالطبع) . ويخرج لدينا النص المشفر :

$$E = AP = \begin{pmatrix} 18 & 17 & 24 & 8 & 1 & 1 & 3 & 1 & 13 \\ 12 & 6 & 3 & 1 & 17 & 6 & 23 & 24 & 2 \end{pmatrix}$$

الآن نقوم بتحويل هذه القيم إلى أعداد .

$$E = AP = \begin{pmatrix} R & Q & X & H & A & A & C & A & M \\ L & F & C & A & Q & F & W & X & B \end{pmatrix}$$

ونقوم بترتيبها بعد ذلك ، ويخرج لدينا النص المشفر التالي :
RLQFXCHAAQAFCWAXMB

الآن لفك التشفير ، نقوم بتجميع الحروف المشفرة في بلوك مكون من حرفين (كما في التشفير) ومن ثم نقوم بضرب المصفوفة في معكوس المصفوفة ، ويخرج لدينا النص الأصلي (طبعا تذكر أخذ باقي القسمة على 26 في حاله كان العدد الناتج أكبر من 26 . لماذا نقوم بذلك دائما ؟ الجواب ببساطه لأننا نريد حصر الناتج في نطاق الحروف الأبجدية ، فإذا كانت الأبجدية تتكون من N حرف اذا سوف نأخذ باقي القسمة على n وهو ما يعرف بـ **modular arithmetic**).

الآن بضرب المعكوس في النص المشفر ، وأخذ الناتج 26 mod ، يخرج لدينا :

$$D = A^{-1} E = \begin{pmatrix} 20 & 5 & 18 & 6 & 19 & 15 & 9 & 5 & 9 \\ 8 & 16 & 15 & 5 & 19 & 18 & 19 & 22 & 12 \end{pmatrix}$$

ونقوم بتحويله إلى أحرف : ليخرج لدينا :
THE PROFESSOR IS EVIL
وهو النص الأصلي

على العموم طريقه التشفير هذه ضعيفة أيضا وخاصة لطريقه **row reduction** حيث تستطيع كسر هذه الشفره ببساطة ، وسوف نتطرق لها في النسخة القادمة بإذن الله) .

PDF created with pdfFactory Pro trial version www.pdffactory.com