سوف نذكر اشهرها ، على العموم في حال استخدمنا أي طريقه يجب أن تكون مفهومه للشخص الذي نريده أن يفك تشفير الرسالة أي يعرف هذه البايتات هي بايتات اضافيه.

الطريقه الأشهر للحشو : هي أن نعرف أولا عدد البايتات التي سوف نضيفها إلى الكتلة الناقصة ، في المثال السابق كانت (13 بايت) ، بعدها نقوم بتكرار هذا العدد في كل بايت في الكتلة ، أي انه سنحشو العدد "13" ثلاثة عشر مره ، وتسمى هذه الطريقه **PKC#5**

في عمليه فك التشفير ، سننظر إلى الكتلة الاخيره ونرى إن كان هناك عدد ما يتكرر في كل خانه من خانات الكتلة الاخيره ، ومنه سوف نعرف هل كان هناك حشو أو لا .

طبعا عند التشفير ، في حاله الكتلة الاخيره تساوي 16 بايت فلا يوجد داعي للحشو (أصلا لا يوجد مكان للحشو).

المشكلة في هذا النوع "شفره الكتل " Block Cipher هو انه في حاله كانت هناك كلمات تتكرر كثيرا في النص الأصلي ، فإنها بعد التشفير سوف يكون النص المشفر متشابه أيضا .

مثلا الاسم " wajdy essam " ظهر 3 مرات في مواقع مختلفة في النص الأصلي (أو الرسالة) . مثلا ظهر في الكتلة الأولى (أول 16 بايت) والكتلة الرابعة (رابع 16 بايت) والكتلة العاشر(عاشر 16 بايت).

الآن عند التشفير ،
دخلت الكتلة الأولى "Wajdy Essam" وتتشفر إلى "Selrurjgqm"
دخلت الكتلة الرابعة "Wajdy Essam" وتتشفر إلى " Selrurjgqm "
دخلت الكتلة العاشرة "Wajdy Essam" وتتشفر إلى " Selrurjgqm "

نلاحظ انه يمكن للمخترق معرفه أن الثلاثة " Selrurjgqm " هي عبارة عن جمله واحده ، وهنا ممكن أن يكسرها بسهوله .

الحل لتجنب مثل هذا التكرار هو استخدام أساليب تسمى" **Mode Of Operation** أنماط أو أساليب العمليات" والبعض يطلق عليها **Feedback Modes** سنتناول هذه الأساليب في النسخة النهائية من الكتاب .

على العموم اشهر هذه الأساليب هو **cipher block chaining** اختصارا (**CBC**) ، هنا في هذا النمط سوف نطبق العملية XOR في النص الأصلي الحالي و النص المشفر السابق .

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