شيفرة بادانين

أوهاج بادانين عمر
ماجستير تمويل ومحاسبة

التشفير هو عبارة عن ممارسة حماية المعلومات باستخدام الخوارزميات المشفرة وعلامات التجزئة والتوقيعات. يمكن أن تكون المعلومات غير نشطة (مثل ملف على القرص الصلب)، أو متنقلة (مثل الاتصالات الإلكترونية المتبادلة بين طرفين أو أكثر)، أو قيد الاستخدام (أثناء الحوسبة على البيانات).

إن للتشفير أربعة أهداف أساسية[1]:

- السرية – إتاحة المعلومات للمستخدمين المصرح لهم فقط.
- النزاهة – ضمان عدم التلاعب بالمعلومات.
- المصادقة – تأكيد صحة المعلومات أو هوية المستخدم.
- عدم الانكار – منع المستخدم من إنكار الالتزامات أو الإجراءات السابقة.

ما المقصود بتشفير المفتاح المتماثل؟

تستخدم خوارزميات تشفير المفتاح المتماثل مفاتيح التشفير نفسها لتشفير النص العادي وفك تشفير المعلومات المشفرة على حد سواء. ويستلزم التشفير المتماثل حصول جميع مستلمي الرسائل المقصودين على حق الوصول إلى مفتاح مشترك.

ما المقصود بالتشفير غير المتماثل (المفتاح العام)؟

يتكون التشفير غير المتماثل أو المفتاح العام من مجموعة كبيرة من الخوارزميات. وتستند على هذه المجموعة مسائل رياضية يسهل أداؤها نسبيًا في اتجاه واحد، ولكن لا يمكن عكسها بسهولة.

هذا المنتج يحتاج لمعادلات لبناء الشيفرة بواسطة المرسل وكذلك على معادلات فك الشيفرة لذا يتطلب النظام نافذة لبناء الشيفرة ونافذة أخرى لفك الشيفرة على فرضية عمل النظام ببرنامج اكسس.

معادلات بناء الشيفرة بالنسبه للمرسل:

المعادلة الاولى:

[1] aws

اذا كانت لغة التشفير باللغة العربية :

ص = ك ط + ٢٨ ك ف – (٢٨ ك + (ك ÷ ٢))

وإذا كانت لغة التشفير باللغة الانجليزية :

ص = ك ط + ٢٦ ك ف – (٢٦ ك + (ك ÷ ٢))

حيث أن :

ك تمثل عدد حروف اسم المرسل إليه .

ط تمثل ترتيب الحرف فى اللغة .

ف يمثل ترتيب المجموعة التي يقع فيها الحرف (للتوضح أكثر فإن الترتيب يقع فى المجموعة الأولى وإلى مالا نهاية) .

المعادلة الثانية لايجاد قيمة (ن) :

ن = ((ص ÷ ع) – ١) ÷ ٢

حيث أن ع تمثل مجموع الشيفرة بالنسبة للحرف المشفر حسب الترتيب شفرات المرسل، بمعنى أن المرسل أرسل عشرات الشفرات (ع هنا الشيفرة رقم ٤ لأن اسم المرسل إليه محمد أي حروف محمد أربعة أحرف) .

المعالة الثالثة لايجاد قيمة (س) :

س = ((((ص – (ك ÷ ٢)) ÷ ك) – ن) (ك) + (ك ÷ ٢)) ÷ (ك ÷ ٢)

الشفرات المرسلة للمستقبل من الراسل .

اسم المرسل إليه أو أي اسم يتفق عليه

وبغرض ايجاد قيمة (ك ، ع)

الشفرات المرسلة لكل حرف مشفر تتكون من الأرقام المتمثلة فى قيم ن ، س ، ف

معادلات فك الشيفرة

ص = (((س – ١) ÷ ٢ + ن) (ك) + (ك ÷ ٢)

ط = (ص + (٢٨ ك ÷ (ك ÷ ٢)) – ٢٨ ك ف) ÷ ك

وبعد الحصول على قيمة (ط) يظهر اسم الحرف المشفر .

مثال لتشفير الحرف (و) الذي يقع فى المجموعة الأولى

الشخص المرسل إليه على :

ف = ١

ك = ٣

ع = ٥

تشفير (و)

ترتيب الحرف (و) = ٢٧

ط = ٢٧

ص = ٨١ + ٨٤ – (٨٤ + ١.٥٠) = ٧٩.٥

ن = ((ص ÷ ع) – ١) ÷ ٢

ن = ((٧٩.٥ ÷ ٥) – ١) ÷ ٢

ن = ٧.٤٥

س = ((((ص – (ك ÷ ٢)) ÷ ك) – ن) (ك) + (ك ÷ ٢)) ÷ (ك ÷ ٢)

س = ((((٧٩.٥ – (٣ ÷ ٢)) ÷ ٣) – ٧.٤٥) (٣) + (٣ ÷ ٢)) ÷ (٣ ÷ ٢)

س = ٣٨.١

الشفرة المرسلة للمستقبل

ن . س. ف (٧.٤٥ ، ٣٨.١ ، ١)

معادلات فك الشيفرة عند المستقبل :

ص = (((س – ١) ÷ ٢) + ن) (ك) + (ك ÷ ٢)

ط = (ص + (٢٨ ك + (ك ÷ ٢)) – ٢٨ ك ف) ÷ ك

بعد الحصول على قيمة (ط) يظهر اسم الحرف المشفر

فك الشيفرة للحرف (و) (ن = ٧.٤٥ ، س = ٣٨.١ ، ف = ١)

ص = (((س – ١) ÷ ٢) + ن) (ك) + (ك ÷ ٢)

ص = (((٣٨.١ – ١) ÷ ٢) + ٧.٤٥) (٣) + (٣ ÷ ٢) = ٧٩.١

ط = (ص + (٢٨ ك + (ك ÷ ٢)) – ٢٨ ك ف) ÷ ك

ط = (٧٩.٥ + (٨٤ + (١.٥)) – ٨٤) ÷ ٣ = ٢٧

بما ان (ط) ترتيب الحرف وهو ٢٧ يقابله الحرف (و)

مثال لتشفير الحرف (و)ويقع فى المجموعه الثالثة

الشخص المرسل اليه على

ف = ٣

ك = ٣

ع = ٥

تشفير (و)

ترتيب الحرف (و) = ٢٧

ط = ٢٧

ص = ٨١ + ٢٥٢– (٨٤ + ١.٥٠) = ٢٤٧.٥

ن = ((ص ÷ ع) – ١) ÷ ٢

ن = ((٢٤٧.٥ ÷ ٥) – ١) ÷ ٢

ن = ٢٥.٢٤

س = ((((ص – (ك ÷ ٢)) ÷ ك) – ن)(ك) + (ك ÷ ٢)) ÷ (ك ÷ ٢)

س = ((((٢٤٧.٥ – (٣ ÷ ٢)) ÷ ٣) – ٢٥.٢٤)(٣) + (٣ ÷ ٢)) ÷ (٣ ÷ ٢)

س = ١١٦.٥

الشفرة المرسله للمستقبل

ن . س. ف (٢٥.٢٤، ٣١١٦.٥)

معادلات فك الشيفرة عند المستقبل

ص = (((س – ١) ÷ ٢) + ن)(ك) + (ك ÷ ٢)

ط = (ص + (٢٨ ك + (ك ÷ ٢)) – ٢٨ ك ف) ÷ ك

بعد الحصول على قيمة (ط) يظهر اسم الحرف المشفر

فك الشيفرة للحرف (و) (ن = ٧.٤٥، س = ٣٨.١، ف = ١)

ص = (((س – ١) ÷ ٢) + ن) (ك) + (ك ÷ ٢)

ص = (((١١٦.٥ – ١) ÷ ٢) + ٢٥.٢٤) (٣) + (٣ ÷ ٢) = ٢٤٧.٥

ط = (ص + (٢٨ ك + (ك ÷ ٢)) – ٢٨ ك ف) ÷ ك

ط = (٢٤٧.٥ + (٨٤ + (١.٥)) – ٢٥٢) ÷ ٣ = ٢٧

بما أن (ط) ترتيب الحرف وهو ٢٧ يقابله الحرف (و) .