

بسم الله الرحمن الرحيم
والصلاة والسلام على أشرف المرسلين
سيدنا محمد صلى الله عليه وسلم



دراسة مبسطة حول :

RSA Encryption I

By :

WoLFGanG / AT4RE

الفهرس:

1. مقدمة -
2. RSA في الرياضيات المستخدمة في -
3. Euler's Theorem (قانون أولر) -
4. خوارزمية الـ RSA -

ملاحظة 1: لاستيعاب النص جيدا من المستحسن طباعته 6

ملاحظة 2: يستحسن كذلك تطبيق الأمثلة المدمجة مع الدرس !

ملاحظة 3: الدرس منقول ومترجم عن أحد أعضاء FOFF لذا عذرا ان كان هناك أخطاء ©

مقدمة:

RSA هي خوارزمية لتشفير النصوص ذات مفتاح خاص, معناه هناك شخص يمتلك مفتاح خاص الذي بواسطته يقوم بفك تشفير النصوص ويقوم بتزويد أشخاص آخرين بمفتاح عام, بحيث يستطيع الشخص الذي يمتلك المفتاح العام بتشفير النص أو المعلومات المراد إرسالها إلى المستقبل الذي يمتلك المفتاح الخاص.

ملاحظة: لا يستطيع فك تشفير النص إلا من يمتلك المفتاح الخاص.



شرح بعض التعاريف الرياضية المستخدمة في الـ RSA :

mod: وهذا الرمز معناه رياضيا باقي حاصل قسمة عددين

(Exponentiation) القوة النونية لعدد :

ومعناه أن نأخذ عدد ونرفعه لقوة عدد آخر و تكتب هكذا

$$2^3 = 2 * 2 * 2 = 8$$

Mod Exponentiation: هو باقي حاصل القسمة النونية وهو من

العمليات الأساسية التي نستعملها كثيرا في هذه الخوارزمية ويكتب هكذا:

$$x^y \text{ mod } z$$

x: هو النص الخام / او المراد تشفيره

Y: المفتاح

Z: القاسم

نتيجة هذه العملية (Pmod): نص مشفر (Cyphered Text) .

مثال بسيط :

لنقم بتشفير الأرقام من 1 إلى 5

المفتاح = 5

القاسم = 50

$$\begin{aligned}1^5 \bmod 50 &= 1 \\2^5 \bmod 50 &= 32 \\3^5 \bmod 50 &= 43 \\4^5 \bmod 50 &= 24 \\5^5 \bmod 50 &= 25 \\&\cdot \\&\cdot \\&\cdot \\11^5 \bmod 50 &= 1\end{aligned}$$

نلاحظ أن باقي حاصل القسمة النونية للعددين 1 و 11 هو نفسه العدد 1
لو اعتمدنا هذه الطريقة للتشفير سوف يقع لدينا خلط بين بعض الحروف
إذا سوف نتوسع أكثر.

Euler's Theorem (قانون أولر):

نص القانون:

$$X^{\phi(Z)} \bmod Z = 1$$

$\phi(Z)$ هو Euler's Totient (لا اعرف شرحها باللغة العربية), لكن معناها إذا كان
 Z موجب فإن النتيجة ستكون حتميا مجموعة الأعداد الصحيحة الموجبة الأقل من أو تساوي
العدد Z والتي هي أولية (Coprime) مع العدد n .

بعض الخواص:

1- الأعداد الأولية فيما بينها هي التي القاسم المشترك بينها العدد 1.
مثلا : 7 و 8 أوليان فيما بينهما, 7 و 14 ليسا أوليان فيما بينهما.

2- أي عدد أولي له لا يقبل إلا القسمة على نفسه و على العدد 1

3- الدالة $\phi(Z)$ هي بكل بساطة مجموعة أو عدد الأرقام الأولية مع Z
بحيث إذا كان z أولي فإن $\phi(Z)$ ستكون بكل بساطة $z-1$

لنرى على مثال لنفهم أكثر:

نأخذ الرقم 7 (أولي):	
1 هو أولي مع العدد 7	≤ 1
2 هو أولي مع العدد 7	≤ 2
3 هو أولي مع العدد 7	≤ 3
4 هو أولي مع العدد 7	≤ 4
5 هو أولي مع العدد 7	≤ 5
6 هو أولي مع العدد 7	≤ 6
$6 = 1-7 = 1-z = (z)\phi$	

نأخذ الرقم 6 (ليس أولي):	
1 هو أولي مع العدد 6	≤ 1
2 هو ليس أولي مع العدد 6	
3 هو ليس أولي مع العدد 6	
4 هو أولي مع العدد 6	≤ 2
5 هو أولي مع العدد 6	≤ 3
$1-Z \neq (z)\phi$ لكن تساوي 3	

لنرجع الآن إلى نظرية أولر :

$$X^{\phi(Z)} \bmod Z = 1 \bmod z$$

لنرى مثال آخر:

لنأخذ العدد 2 ونأخذ $Z = 7$ إذا نرفع 2 إلى القوة 6 ونقسمه على العدد 7 نحصل دائما على باقي يساوي 1 .

نحن نعلم أن إذا كان $X=Y$ فإن $X*X=Y*Y$. أو $X=Y$ فإن $X*X=Y*X$. هذا يعني:

$$X^{\phi(Z)} \bmod Z * X^{\phi(Z)} \bmod Z = 1 \bmod z * 1 \bmod z$$

لنختصر قليلا:

$$X^{(2*\phi(Z))} \bmod Z = 1*1 \bmod z$$

نلاحظ أن النتيجة هي نفسها دائما مهما كررنا الأمر :

$$X^{(3*\phi(Z))} \bmod Z = 1*1*1 \bmod z$$

$$X^{(4*\phi(Z))} \bmod Z = 1*1*1*1 \bmod z$$

$$X^{(5*\phi(Z))} \bmod Z = 1*1*1*1*1 \bmod z$$

⋮

$$X^{(W*\phi(Z))} \bmod Z = 1*1*1*1*...*1 \bmod z$$

لدينا الآن معادلة رياضية التي بواسطتها رفعنا X (الذي هو نصنا المراد تشفيره) الى أي مضاعف للدالة $\phi(Z)$ نصل دائما على نفس العدد 1.

لكن هذا غير كاف.

لنحاول ضرب كلا الطرفين في العدد X

$$X^{(W*\phi(Z)) \bmod Z} * X = 1 * 1 \bmod z * X$$

نختصر الى:

$$X^{(W*\phi(Z)+1) \bmod Z} = X \bmod z$$

اعتمادا على السابق لدينا :

$$X^{(Z-1) \bmod Z} = 1$$

و

$$X^{(Z-1)} * X \bmod Z = 1 * X \bmod Z$$

و منه نستنتج:

$$X^{(Z) \bmod Z} = X \bmod Z$$

نستبدل الحروف بالارقام لنوضح أكثر:

$$2^{(7-1) \bmod 7} = 1$$

و

$$2^{(7) \bmod 7} = 2$$

هذا جيد جدا, لكن غير كاف كذلك لاستعماله في التشفير, لذا سنبحث أكثر:
لدينا الدالة ϕ لجداء عددين أوليين P و q هو جداء الدالة ϕ لكلا العددين أي:

$$\phi(p*q) = \phi(p) * \phi(q) = (p-1) * (q-1)$$

مثال:

لنأخذ عددين أوليين: $p=83$, $q=53$

$$p*q=4399$$

$$p-1 * q-1 = 4264$$

$$\phi(p*q)=p-1 * q-1 =4264$$

لنجرب الآن تغيير المتغير Z بالرقم $(p*q)$ تصبح العبارة كالتالي:

$$X^{\phi(p*q) \bmod p*q} = 1 \bmod (p*q)$$

نحن نعلم أن العبارة $\phi(p \cdot q)$ تصبح $(p-1) \cdot (q-1)$ لأن P و q أوليان فتصبح العبارة كالتالي:

$$X^{(p-1) \cdot (q-1) \bmod p \cdot q} = 1$$

أو باستعمال الأرقام:

$$X^{2264 \bmod 4399} = 1 \pmod{4399}$$

باستعمال p و q اللذين هما عددين أوليين:

$$10^{2264 \bmod 4399} = 1$$

$$20^{2264 \bmod 4399} = 1$$

$$30^{2264 \bmod 4399} = 1$$

الآن نصل إلى أهم جزء من خلال ما قمنا به سابقاً:

$$X^{\phi(Z)} \cdot X \bmod Z = 1 \cdot X \pmod{z}$$

هي نفسها:

$$X^{\phi(Z) + 1} \bmod Z = 1 \cdot X \pmod{z}$$

الآن عندما نضع $z = p \cdot q$ عندها يكون $\phi(Z) = \phi(p \cdot q) = (p-1) \cdot (q-1)$ ومنه:

$$X^{\phi(p-1 \cdot q-1)} \cdot X \bmod Z = X \pmod{z}$$

وبتطبيق خواص الأس نختر العبارة الى :

$$X^{\phi((p-1) \cdot (q-1) + 1) \bmod Z} = X \pmod{z}$$

إذن عندما نضيف 1 إلى الأس و نطبق التغيرات على المثال السابق:
لاحظ جيداً الفرق

$$10^{2265 \bmod 4399} = 10$$

$$20^{2265 \bmod 4399} = 20$$

$$30^{2265 \bmod 4399} = 30$$

خوارزمية الـ RSA:

الآن نحن مستعدون لشرح كيف تحصلنا على خوارزمية التشفير من المعدلات السابقة , المعادلة السابقة مهمة جداً بحيث نستطيع ان نرى حالياً أن النص المراد تشفيره $P = (10, 20, 30)$ نستطيع الحصول عليه ثانية بتطبيق المعادلة التالية كما في المثال السابق :

$$P^{2265 \bmod 4399}$$

نستطيع الان ان نقسم المعادلة السابقة الى معادلتين:

معادلة تشفير و معادلة فك تشفير

عندها نحتاج الى مفتاح تشفير (e) و مفتاح فك تشفير (d)
نبدأ الان مع E والذي يجب ان يكون أولي مع $(p-1)*(q-1)$
لنختار مثال:

لدينا 3 هو أولي مع 4265 إذن 3 سيكون E

إذا اردنا ان نحسب d سيتوجب علينا ان نقوم بالعملية العكسية :

$E^{-1} \bmod (p-1)*(q-1)$ هنا سيتوجب علينا الحصول على آلة حاسبة جيدة
إذن:

$$3^{-1} \bmod 4265 = 2843 \text{ (d)}$$

هنا سيكون لدينا 3 هو مفتاح التشفير و 2843 هو مفتاح فك التشفير.

أخيرا , القانون العم لـ RSA:

$$C = P^E \bmod m$$
$$P = C^D \bmod m$$

حيث :

C: Cyphered Text (النص المشفر)

P: Plain Text (النص المراد تشفيره)

E: Encryption Key (مفتاح التشفير)

D: Decryption Key (مفتاح فك التشفير)

m: modulus

مثال :

لنجرب تشفير النص: 1000

$$1000^E(3) \bmod m(4399) = C(1724)$$
$$1000 \rightarrow 1724$$

لنفك تشفير هذا النص:

$$1724^D(2843) \bmod m(4399) = C(1000)$$
$$1724 \rightarrow 1000$$

ملاحظة :

P يجب أن يكون أقل من m, لهذا يجب أن يكون m عدد أولي كبير نوعا ما وهذا لضمان الحماية.