فصل– 6 التشفير بالمفتاح المعلن

6.1 مقدمة عن التشفير بالمفتاح المعلن

قدّم التشفير بالمفتاح المعلن public key ثورة في مجال التشفير. لحين ذلك الوقت ، كان التشفير يعتمد بصورة مكثفة على استخدام المفاتيح السرية لاتمام التواصل السرّي مما يستدعي عقد لقاءات سرية للاتفاق على تلك المفاتيح وهذه المشكلة تعرف بمشكلة **توزيع المفاتيح** key distribution problem. في المقابل ، حلّ التشفير بالمفتاح المعلن هذه المشكلة ، وذلك بتمكين اي طرفين من التواصل الخاص بدون الحاجة للاتفاق المسبق على اي معلومة سرية.

- في اطار التشفير بالمفتاح الخاص ، يتفق طرفان على المفتاح k لاستخدامه في عمليتي التشفير وفك الشفرة.
- اما في اطار التشفير بالمفتاح المعلن ، يولّد المستلم receiver زوج من المفتايح (pk, sk) تعرف بالمفتاح المعلن والمفتاح الخاص ، على التوالي.
- يستخدم الطرف المرسل sender المفتاح المعلن pk لتشفير الرسالة. اما المستلم فيستخدم المفتاح الخاص sk لفك شفرة الرسالة المستلمة.
- وبما ان الهدف هو منع الحاجة لعقد لقاء مسبق بين الطرفين للاتفاق على المفتاح ، يقوم الطرف المستلم بارسال مفتاحه المعلن pk الى الطرف المرسل بصورة صريحة ، او يعلن ذلك المفتاح في مكان عام (كصفحة الويب ، مجلة ، بطاقة تعريف ،...الخ) بحيث يتمكن اي طرف مرسل من استخدام ذلك المفتاح للتواصل مع الطرف المستلم. تحت هذا الاطار ، يستطيع عدة اطراف استخدام المفتاح المعلن للمستلم في نفس الوقت لكي يتواصلوا مع صاحب ذلك المفتاح. هذه الخاصية تختلف عن اطار التشفير بالمفتاح الخاص الذي يحتم استخدام مفاتيح خاصة مختلفة لكل زوج من الاطراف لكي يتواصلوا مع بعضهم البعض.
- من المهم الاشارة الى ان خصوصية التشفير بالمفتاح المعلن لاتعتمد على المفتاح المعلن ، وذلك لكونه معلن ويستطيع الخصم الوصول اليه ، بل تعتمد الخصوصية على المفتاح الخاص sk لذا يتحتم على صاحب هذا المفتاح (المستلم) عدم كشفه لاي طرف اخر بما فيهم المرسل. وبما ان مفتاح التشفير يختلف عن مفتاح فك الشفرة فإن منهج التشفير بالمفتاح المعلن يعرف **بالتشفير غير المتناظر** Asymmetric.
- عندما يتواصل المستلم مع U من المرسلين ، في اطار التشفير بالمفتاح المعلن ، فانه يحتاج الى خزن مفتاحه الخاص فقط sk بدلا من خزن وادارة U من المفاتيح. اما في حالة التشفير بالمفتاح الخاص فكل طرف يحتاج الى تخزين U من المفاتيح الخاصة. وهذا يوضّح مرونة التشفير بالمفتاح المعلن مقارنة مع التشفير بالمفتاح الخاص من حيث خزن وادراة المفاتيح.
- السلبية الوحيدة لمناهج التشفير بالمفتاح المعلن هي انها ابطأ بمقدار مرة او مرتين من مناهج التشفير بالمفتاح الخاص وذلك لانها تعتمد على عمليات رياضية معقدة ، مما يجعل استخدامها يمثل تحديا بالنسبة للاجهزة محدودة الموارد كالبطاقات الذكية smartcards. في حقيقة الامر ، يمكن استخدام مناهج التشفير بالمفتاح الخاص لتحسين كفاءة مناهج التشفير معلنة المفتاح لتشفير الرسائل الطويلة كما سنرى في الجزء (6.3).

6.2 تعريف التشفير بالمفتاح المعلن

يتكون منهج التشفير بالمفتاح المعلن من ثلاث خوارزميات (Gen, Enc, Dec):

1. تأخذ خوارزمية **Gen** معامل الأمنية n وتولّد المفتاحين (pk, sk) المعلن والخاص ، كل مفتاح طوله اكبر او يساوي n.
2. تأخذ خوارزمية **Enc** المفتاح المعلن pk والرسالة m وتخرج النص المشفّر c ويكتب بالشكل $c \leftarrow Enc_{pk}(m)$.
3. تأخذ خوارزمية **Dec** المفتاح الخاص sk والنص المشفّر c وتخرج الرسالة m او رمز الفشل $\perp$. نفترض ان Dec تعمل بطريقة محددة deterministic $m = Dec_{sk}(c)$.

يجب ان يكون لجميع قيم n ، لكل (pk, sk) من Gen ، ولكل رسالة m فإن $Dec_{sk}(Enc_{pk}(m)) = m$ يكون متحققا.

الأمنية تجاه مهاجمة CPA. كما ذكرنا فإن الخصم يستطيع الوصول للمفتاح المعلن pk مما يعطيه امكانية الوصول "المجاني" لخوارزمية التشفير بحيث يستطيع ان يشفّر اي رسالة من اختياره بحساب $Enc_{pk}(m)$ وهذا يتطابق مع تعريف الأمنية تجاه CPA الذي ذكرناه مسبقا في اطار التشفير بالمفتاح الخاص (راجع جزء 3.3.1). وبالتالي يمكن صياغة التشفير بالمفتاح المعلن اعتمادا على التجربة التالية.

افترض منهج التشفير $\pi = (Gen, Enc, Dec)$ والخصم $\mathcal{A}$

تجربة التمييز من نوع CPA $\mathbf{Pub}^{\mathbf{cpa}}_{\pi,\mathcal{A}}(\mathbf{n})$:

1. Gen تولّد المفاتيح (pk, sk).
2. يعطى الخصم $\mathcal{A}$ المفتاح المعلن pk والوصول الى $Enc_{pk}(.)$. يقوم الخصم باختيار نصيّن صريحين $m_0, m_1 \in \mathcal{M}$ لهما نفس الطول.
3. يقوم المتحدي باختيار الثنائية العشوائية $b \leftarrow \{0,1\}$ ، يشفّر النص $c \leftarrow Enc_{pk}(m_b)$ ويرسل نص التحدي الناتج الى الخصم.
4. يصل الخصم $\mathcal{A}$ الى خوارزمية Enc ويخرج الثنائية b'.
5. يكون اخراج التجربة 1 اذا كان $b = b'$ ، و 0 ماعدا ذلك. يكتب اخراج التجربة $Pub^{cpa}_{\pi}(\lambda) = 1$ اذا كان اخراجها 1 ، وهو يمثل نجاح الخصم.

تعريف(6.1): يكون منهج التشفير π امنا تحت مهاجمة CPA اذا كان لجميع الخصوم $\mathcal{A}$ توجد دالة ضئيلة $negl$ بحيث يتحقق:

$$\Pr\left[\mathrm{Pub}^{\mathrm{cpa}}_{\pi,\mathcal{A}}(n) = 1\right] \leq \frac{1}{2} + \mathrm{negl}(n)$$

وواضح من التعريف اعلاه ، انه لكي يقاوم منهج التشفير بالمفتاح المعلن مهاجمة CPA فيجب ان لايكون محددا deterministic بل يجب ان يكون التشفير من النوع الاحتمالي probabilistic بمعنى ان تشفير نفس الرسالة عدّة مرات يعطي نتائج مختلفة في كل مرة (لإعتماد خوارزمية التشفير على عنصر عشوائي اضافة الى الرسالة المطلوب تشفيرها). يستطيع الخصم في حالة التشفير المحدّد ، عند استلام نص التحدي c ، ان يقارنه مع $Enc_{pk}(c_1)$ و $Enc_{pk}(c_2)$ وينجح بالتجربة باحتمالية 1.

نؤكد هنا ، ان التشفير بالمفتاح المعلن لا يوفّر أمنية تجاه مهاجة من نوع ciphertext only attack ولا يوفّر مستوى الأمنية التامة perfect security اطلاقا كما هو الحال في التشفير بالمفتاح الخاص. والسبب في ذلك كله يرجع الى وصول الخصم الى خوارزمية $Enc_{pk}(.)$ وبالتالي يستطيع الخصم تشفير جميع النصوص الصريحة المحتملة ومقارنتها مع النص المشفر لحين الوصول الى تطابق.

6.3 التشفير الهجين

لزيادة كفاءة التشفير بالمفتاح المعلن يتم دمجه مع التشفير بالمفتاح الخاص للحصول على منهج **تشفير هجين** hybrid encryption يجمع بين مزايا المنهجين. وتتلخص فكرة المنهج الهجين بتقسيم عملة التشفير لى خطوتين:

1. يقوم المرسل اولا باختيار مفتاح سري عشوائي k ، يشفّر ذلك المفتاح السري بالمفتاح المعلن للمستلم. يدعى النص المشفر c_1. يستطيع المستلم استرجاع المفتاح السري k بفك شفرة c_1 ، وبذلك فإن k يبقى غير معروف بالنسبة للخصم كونه محميا بمنهج التشفير المعلن. وهذا يعني تأسيس سر مشترك بين المرسل والمستلم.

2. يعمل المرسل بعدها على تشفير الرسالة m باستخدام منهج التشفير بالمفتاح الخاص وباستخدام المفتاح السري k الذي سبق وان تم مشاركته. تدعى نتيجة التشفير c_2 والتي يمكن فك شفرتها باستخدام المفتاح السري k.

يمكن جمع الخطوتين اعلاه سويا بحيث ينقل المرسل نص مشفّر واحد (c_1, c_2) للمستلم. يتم صياغة التشفير الهجين شكليا بالمنهج (6.1).

Construction (6.1): Hybrid encryption

Let $\pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be public key encryption scheme, let $\pi' = (\text{Enc}', \text{D}')$ be private key encryption scheme. Define $\pi^{hy} = (\text{Gen}^{hy}, \text{Enc}^{hy}, \text{Dec}^{hy})$ as follows:

Gen^{hy}: run Gen.

$\text{Enc}^{hy}_{pk}(m)$: works as follows:

1. Choose $k \leftarrow \{0,1\}^n$ randomly, where n is obtained from pk.
2. Calculate: $c_1 \leftarrow \text{Enc}_{pk}(k)$, $c_2 \leftarrow \text{Eec}'_k(m)$.
3. Output: (c_1, c_2).

$\text{Dec}^{hy}_{sk}(\langle c_1, c_2 \rangle)$: works as follows:

1. $k = \text{Dec}_{sk}(c_1)$.
2. output $m = \text{Dec}'_k(c_2)$.

تكون كفاءة المنهج الهجين افضل عندما يكون $|m| > n$ ، وبخلاف ذلك فانه يكون من الافضل تشفير الرسالة بمنهج التشفير معلن المفتاح. بصورة ادق ، ليكن σ هو كلفة تشفير المفتاح الخاص k وليكن ρ كلفة تشفير الرسالة m ، فإن كلفة تشفير الرسالة التي طولها t باستخدام التشفير الهجين هي:

$$\frac{\sigma + \rho . t}{t} = \frac{\sigma}{\rho} + \rho$$

والتي تقترب من الكلفة ρ (كلفة التشفير خاص المفتاح) عندما يزاد الطول t. وبالتالي فإن التشفير الهجين يجمع بين "وظيفة" التشفير معلن الفتاح و"كفاءة" التشفير خاص المفتاح.

بعد ان تم تقديم تعريف التشفير معلن المفتاح نبدأ الأن بعرض المناهج التي تحقق هذا التعريف. تعتمد هذه المناهج على مفاهيم رياضية من نظرية الاعداد number theory ، ونظرية الزمر التي تم التطرق لها في فصل 6.

6.4 منهج RSA للتشفير

يعتمد منهج تشفير RSA على افتراض RSA الذي ذكرناه في الفصل السابق. المنهج الذي سنذكره هو منهج مناسب للتعليم وغير مناسب ليكون تطبيقيا وذلك لكون التشفير به يكون محددا deterministic وبالتالي يكون غير أمن.

Construction (6.2): RSA encryption scheme

$\mathrm{Gen}(n)$: run $\mathrm{GenRSA}(n)$ to get (N, e, d), where $< N, e >$ is the public key, pk,and $< N, d >$ is the private key, sk.

$\mathrm{Enc}_{pk}(m)$: takes pk and message $m \in \mathbb{Z}_N^*$ and compute:

$$c = [m^e \bmod N].$$

$\mathrm{Dec}_{sk}(c)$: takes sk and cipher text $c \in \mathbb{Z}_N^*$ and computes: $m = [c^d \bmod N]$.

- بالرغم من عدم أمنية هذا التصميم الّا انه يوضّح كيفية استخدام مسألة RSA في تصميم مناهج تشفير معلنة المفتاح كما يمثل مدخلا للمناهج الآمنة الاخرى.
- يوضّح المنهج (6.2) منهج RSA للتشفير.
- يتضح صحة عمل هذا التصميم من خلال متلازمة (5.4).
- يعتبر المنهج (6.2) غير أمن بالنسبة لتعريف الأمنية الخاص بنظم التشفير معلنة المفتاح (تعريف (6.1))، حيث يشترط ان تكون مناهج التشفير احتمالية وليست محدّدة.
- بالرغم من ذلك ، يمكن اثبات نوع أمنية "ضعيفة" لهذا المنهج. عند اختيار الرسالة $m \in \mathbb{Z}_N^*$ بصورة عشوائية ، فلا يوجد خصم يستطيع ان يسترجع تلك الرسالة من النص المشفر $c = [m^e \bmod N]$. يستند برهان هذه الأمنية على "مسألة RSA" مباشرة.

مثال(7.1): افترض ان لدى الطرف Bob $p = 101$ ، و $q = 113$. اذن ، $n = 11413$ ،و $\emptyset(n) = 100 \times 112 = 11200$. افترض $e = 3533$ بحيث $\gcd(e, \emptyset(n)) = 1$. عندها يكون $d = e^{-1} \bmod 11200 = 6597$.

يعلن Bob قيم $n = 11413$ ، و $e = 3533$. نفترض الأن ان Alice ترغب بتشفير النص الصريح 9726 لترسله الى Bob. تقوم Alice بحساب

$$9726^{3533} \bmod 11413 = 5761$$

وترسل 5761 عبر قناة الاتصال. عندما يستلم Bob النص المشفر 5761 ، يقوم بفك شفرته وذلك بحساب

$$5761^{6597} \bmod 11413 = 9726$$

6.4.1 دوال الاتجاه الواحد

تعتبر مسألة RSA السابقة نموذجا لتصميم دوال بالاتجاه الواحد one—way functions. تمتاز دوال الاتجاه الواحد بسهولة حسابها ولكن هناك صعوبة في حساب معكوسها مالم تتوفر معلومة تسمى trapdoor. لاحظ ، ان المرسل يقوم بحساب $y = x^e \bmod N$ بسهولة ، في حين تكون عملية حساب معكوسها x صعبة للغاية مالم يتوفر المفتاح d الذي يمثل الوسيلة المساعدة لحساب عكس الدالة $x = y^d \bmod N$.

6.4.2 الجانب العملي لمنهج التشفير RSA

ترميز الرسالة. لكي يتم تشفير الرسالة الرمزية m ، يتم ترميز ثنائيات تلك الرسالة الى عناصر ضمن الزمرة $\mathbb{Z}_N$. في حالة كان العنصر الناتج لاينتمي الى الزمرة $\mathbb{Z}_N^*$ (بمعنى $\gcd(m, N) \neq 1$) فانه بالامكان ايضا فك شفرة ذلك العنصر. على كل حال ، عندما تكون الرسالة m عشوائية فإن احتمال عدم انتمائها الى زمرة $\mathbb{Z}_N^*$ تكون قليلة.

اختيار قيمة e. تحدّد قيمة e سرعة عملية التشفير لكونها تتضمن الرفع للاس بمقدار e. لذا عادة مايتم اختيار قيمة $e = 3$. اختيار هذه القيمة يشترط ان يتحقق: $p, q \neq 1 \bmod 3$. في الواقع ، فإن اختيار $e = 3$ يعرّض RSA لبعض الخروقات التي سنذكرها. فيما يتعلق بقيمة d فانها تحسب من الفتاح e. تعتبر فكرة اختيار قيمة d اولا ومن ثم حساب قيمة e ، لكي تسرّع عملية فك الشفرة ، تعتبر فكرة سيئة. عندما تكون قيمة d صغيرة (مثلا $d < N^{1/4}$) فيمكن مهاجمتها بسهولة بطريقة brute force.

استخدام نظرية الباقي الصينية لفك الشفرة. يقوم الطرف المستلم ، الذي يمتلك المفتاح الخاص ، وبالتالي يعرف عوامل $N = p.q$ ، ان يسرّع عملية فكل الشفرة وذلك باستخدام نظرية الباقي الصينية CRT والتي تنص على ان:

$$[c^d \bmod N] \leftrightarrow (c^d \bmod p, c^d \bmod q)$$

وبالتالي فإن المستلم يحسب النتائج الجزئية:

$$m_p = c^d \bmod p = c^{[d \bmod (p-1)]} \bmod p$$

$$m_q = c^d \bmod q = c^{[d \bmod (q-1)]} \bmod q$$

يتم تحويل الزوج (m_p, m_q) الى عنصر واحد كما يلي:

1. تطبيق خوارزمية اقليدس الموسعة لايجاد X, Y ، بحيث $Xp + Yq = 1$.
2. $p1 = [Yq \bmod N], q1 = [Xp \bmod N]$.
3. احسب $x = [m_p.p1 + m_q.q1] \bmod N$.

مثال(6.2): ليكن $p = 11, q = 23, e = 3$.

بذلك فإن $N = 253, \emptyset(N) = 220, d = 147$. لتشفير الرسالة الثنائية $m = 0111001$ بالمفتاح المعلن $kp = < N = 235, e = 3 >$ فأنه يتم ترميز m بالرقم 57 (عنصر ينتمي للزمرة $\mathbb{Z}_{253}^*$). ثم يتم تشفير الرسالة بحساب: $c = 250$.
لفك شفرة النص المشفّر نحسب ببساطة $m = [250^{147} \bmod 253] = 57$. يمكن ان نفك شفرة النص المشفر بتطبيق نظرية الباقي الصينية بحساب:

$$m_p = 250^{[147 \bmod 10]} \bmod 11 = 8^7 \bmod 11 = 2$$

$$m_q = 250^{[147 \bmod 22]} \bmod 23 = 20^{15} \bmod 23 = 11$$

بما ان $11.(-2) + 1.23 = 1$ ، اذن $X = -2, Y = 1$. ثم نحسب

$$p1 = 1.23 \bmod 253 = 23 \text{ ، } q1 = -2.11 \bmod 253 = 231.$$

وبذلك فإن الرسالة $m = [2.23 + 11.231] \bmod 253 = 57$

6.4.3 مهاجمات على طريقة RSA

يخضع التشفير بطريقة RSA المذكورة في المنهج (6.2) للعديد من المهاجمات.

اولا: مهاجمة مسألة RSA: وذلك بمحاولة تحليل N الى عواملها الاولية كما ذكرنا في مسألة RSA ، فراجع. نقول هنا ، انه من الافضل اختيار قيم p وq بطول 1024 ثنائية ، وبالتالي تكون قيمة n بطول 2048 ثنائية وهو رقم يتعذر تحليله بافضل خوارزميات التحليل الحالية.

ثانيا: عندما يكون $e = 3$ وتكون الرسالة المطلوب تشفيرها $m < N^{1/3}$ فإن تشفير الرسالة لايتضمن اي عملية اختزال بعملية $\bmod$ لان الرقم الصحيح $m^3 < N$. وهذا يعني ان الخصم يستطيع مهاجمة النص المشفر واسترجاع الرسالة m بحساب $m = c^{1/3}$.

ثالثا: بما ان طريقة التشفير RSA هي طريقة محددة deterministic ، يمكن ان نعرف قيمة الرسالة m ، التي لها قيم محتملات قليلة ، من النص المشفر $c = [m^e \bmod N]$ وذلك بمحاولة تشفير جميع قيم m ومقارنة النتائج مع c. عندما تكون $1 < m \leq \mathcal{L}$ فإن وقت المهاجمة اعلاه يكون خطيا مع $\mathcal{L}$.

رابعا: تمتلك طريقة RSA للتشفير خاصية غير مرغوب بها تدعى المطاوعة malleable ، والتي تعني ان الخصم يستطيع تحويل النص المشفّر c الى نص اخر c' بحيث عند فك شفرة c' نحصل على تحويل للنص c. فلو حصل الخصم على النص المشفر $c = m^e$ فانه يحسب نص مشفّر جديد $c' = c.r^e$. عند وصول الخصم لخوارزمية التشفير لفك شفرة c' فانه يحصل على:

$$m' = c'^d = (c.r^e)^d = c^d.r = m^{ed}r = mr$$

يستطيع الخصم الحصول على الرسالة الاصلية عن طريق حساب $m'.r^{1-}$. تعرف المهاجمة اعلاه بمهاجمة CPA ، راجع فصل-1.

6.4.4 RSA المحشوة

يمكن اعادة تصميم منهج RSA للتشفير وذلك بجعلها اكثر أمنية ، بحيث تكون متوافقة مع التعريف (6.1) ومقاومة للمهاجمات التي ذكرناها اعلاه. يعتمد المنهج الجديد ايضا على مسألة RSA.

- احد الافكار البسيطة لانجاز هذه المهمة هي باضافة حشو عشوائي random pad للرسالة قبل تشفيرها.
- تتم عملية الحشو padding وفق معايير متفق عليها.
- من ابرز تلك المعايير هو معيار PKCS #1 v2.1.
- تسمى طريقة الحشو المتبعة بهذا المعيار Optimal Asymmetric Encryption Padding (OAEP).
- في واقع الامر ، تعتبر OAEP طريقة حشو وليست طريقة تشفير مستقلة.
- سوف نجمع بين طريقة OAEP للحشو وطريقة RSA للتشفير.
- تقوم OAEP بحشو الرسالة m التي طولها $n/2$ الى رسالة $\widehat{m}$ بطول $2n$.
- تستخدم OAEP دالتين $h_1, h_2: \{0,1\}^n \to \{0,1\}^n$.
- يوضّح منهج (7.3) التشفير بطريقة RSA-OAEP.

Construction (6.3): RSA–OAEP encryption scheme

Assumptions: $GenRSA$, $h_1, h_2: \{0,1\}^n \to \{0,1\}^n$ be two functions.

Key generation: Run $GenRSA(n+1)$ to obtain

$$< \mathrm{N}, \mathrm{e}, \mathrm{d} >.$$

Encryption: To encrypt the message $\mathrm{m} \in \{0,1\}^{n/2}$, first choose $\mathrm{r} \leftarrow \{0,1\}^n$ randomly, then set $\mathrm{m}' = \mathrm{m}||0^{n/2}$, compute $\widehat{\mathrm{m1}} = h_1(\mathrm{r}) \oplus \mathrm{m}'$, and $\hat{\mathrm{m}} = \widehat{\mathrm{m1}}||(\mathrm{r} \oplus h_2(\widehat{\mathrm{m1}}))$. It outputs the ciphertext $\mathrm{c} = \hat{\mathrm{m}}^{\mathrm{e}} \bmod \mathrm{N}$.

Decryption: To decrypt c, compute $\hat{\mathrm{m}} = \mathrm{c}^{\mathrm{d}} \bmod \mathrm{N}$, and divide $\hat{\mathrm{m}}$ to $\widehat{\mathrm{m1}}||\widehat{\mathrm{m2}}$, where $|\widehat{\mathrm{m1}}| = |\widehat{\mathrm{m2}}| = \mathrm{n}$. Then compute $\mathrm{r} = h_2(\widehat{\mathrm{m1}}) \oplus h_1(\widehat{\mathrm{m2}})$, and get $\mathrm{m}' = \widehat{\mathrm{m1}} \oplus h_1(\mathrm{r})$. If the last $\mathrm{n}/2$ bits of m' are not $0^{n/2}$ then output $\perp$, otherwise output the first $\mathrm{n}/2$ bits of m'.

6.5 منهج El Gamal للتشفير

- يعتبر منهج El Gamal احد مناهج التشفير معلنة المفتاح كثيرة الاستخدام و يعتمد في امنيته على افتراض Decisional Diffie-Hellman (DDH).
- يمتاز منهج El Gamal بكون التشفير فيه احتماليا probabilistic ، وبالتالي ينسجم مع تعريف (6.1) للامنية والذي يقاوم المهاجمات من نوع CPA.

Construction (6.4): El Gamal encryption scheme

$\mathbf{Gen(n)}$: choose the cyclic group $\mathbb{G}$ of order q ($|\mathrm{q}| = \mathrm{n}$), the generator g, and chooses $\mathrm{x} \leftarrow \mathbb{Z}_{\mathrm{q}}$. The public key pk is $< \mathbb{G}, \mathrm{q}, \mathrm{g}, \mathrm{g}^{\mathrm{x}} >$, the secret key sk is $< \mathbb{G}, \mathrm{q}, \mathrm{g}, \mathrm{x} >$.

$\mathbf{Enc_{pk}(m)}$: to encrypt the message $\mathrm{m} \in \mathbb{G}$ with pk, first choose $\mathrm{y} \leftarrow \mathbb{Z}_{\mathrm{q}}$ and output the ciphertext

$$< \mathrm{g}^{\mathrm{y}}, \mathrm{h}^{\mathrm{y}}.\mathrm{m} >.$$

$\mathbf{Dec_{sk}}(< \mathbf{c_1}, \mathbf{c_2} >)$: to decrypt $< \mathrm{c}_1, \mathrm{c}_2 >$ with sk, compute:

$$\mathrm{m} = \mathrm{c}_2 / \mathrm{c}_1{}^{\mathrm{x}}.$$

- يوضّح المنهج (6.4) منهج El Gamal للتشفير.

لنرى كيف ان فك التشفير يعمل بصورة صحيحة ، ليكن

$$< \mathrm{c}_1, \mathrm{c}_2 >=< \mathrm{g}^{\mathrm{y}}, \mathrm{h}^{\mathrm{y}}.\mathrm{m} >$$

حيث $\mathrm{h} = \mathrm{g}^{\mathrm{x}}$. لاحظ بعدها ان:

$$\frac{c_2}{{c_1}^x} = \frac{h^y . m}{(g^y)^x} = \frac{(g^x)^y . m}{g^{xy}} = \frac{g^{xy} . m}{g^{xy}} = m$$

مثال(7.3): افترض $q = 2579$ و$g = 2$. ليكن $x = 765$. عندها يكون

$$h = 2^{765} \bmod 2579 = 949$$

افترض اننا نرغب بتشفير الرسالة $m = 1299$. افترض ان $y = 853$ هي القيمة العشوائية التي نختارها اثناء عملية التشفير. عندها يتم التشفير كما يلي:

$$c_1 = 2^{853} \bmod 2579 = 435,$$

$$c_2 = 1299 \times 949^{853} \bmod 2579 = 2396$$

لفك شفرة النص المشفر $(435,2396)$ فاننا نحسب:

$$m = 2396 \times (435^{765})^{-1} \bmod 2579 = 1299$$

وهو بالفعل الرسالة المرسلة.

6.5.1 التطبيق العملي لطريقة El Gamal

التعامل مع مجاميع رتبتها اولية. يفضّل ان تكون الزمرة التي نتعامل معها في منهج تشفير El gamal هي زمرة ذات رتبة اولية (عدد عناصرها اولي) وهناك عدة اسباب لهذا التفضيل:

السبب الاول: تصعيب حل مسألة اللوغاريتم المتقطع.

السبب الثاني: انه يسهل الحصول على مولّد للزمرة التي رتبتها اولية ، استنادا الى متلازمة (6.4) التي تنص على ان كل عنصر (باستثناء عنصر الوحدة) في زمرة رتبتها عدد اولي فانه مولّد.

بقي الأن معرفة كيفية تحويل الزمرة $\mathbb{Z}_p^*$ التي رتبتها عدد غير اولي $(p-1)$ الى زمرة جزئية بحيث تكون رتبتها عدد اولي.

- $y \in \mathbb{Z}_p^*$ يُدعى بقية تربيعية $\bmod p$ اذا وجد عنصر $x \in \mathbb{Z}_p^*$ بحيث $x = y^2 \bmod p$.
- لاحظ ، ان نصف عناصر الزمرة $\mathbb{Z}_p^*$ هي بقايا تربيعية وهي زمرة جزئية من $\mathbb{Z}_p^*$.
- عندما يكون P هو عدد اولي قوي strong prime ، بمعنى ان $p = 2q + 1$ بحيث q هو عدد اولي ، فإن زمرة البقايا التربيعية تتضمن $\frac{p-1}{2} = q$ من العناصر.
- وبما ان q هو عدد اولي فإن الزمرة الجزئية الناتجة هي زمرة دورية وجميع عناصرها مولدآت ، بالاضافة الى صعوبة حل مسألة اللوغاريتم المتقطع لها بسهولة.

تشفير الرسائل. لغرض التشفير بمنهج El Gamal نحتاج الى تحويل الرسالة m المطلوب تشفيرها الى عنصر ضمن الزمرة $\mathbb{G}$.

- احد الطرق المستخدمة هي باختيار p كعدد اولي قوي بحيث $q = (p-1)/2$ هو ايضا عدد اولي.
- عند هذه الحالة يكون q رتبة الزمرة $\mathbb{G}$ كما ذكرنا قبل قليل.

- يتم تحويل الخيط الرمزي $\widehat{m}$ بطول $n-1$ الى عنصر $m \in \mathbb{G}$ بالطريقة التالية: اولا يتم تحويل الخيط الرمزي الى عدد صحيح ومن ثم يتم اضافة 1 للحصول على العدد الصحيح $1 < \bar{m} \leq q$. بعدها نحسب

$$m = [\bar{m}^2 \bmod p]$$

مثال(7.4): ليكن $q = 83$ ، $p = 2q + 1 = 167$. ليكن $g = 2^2 = 4 \bmod 167$. نفترض ان المفتاح السري هو $37 \in \mathbb{Z}_{83}$ وبذلك فإن المفتاح المعلن هو $pk =< 167,83,4, [4^{37} \bmod 167] >=< 167,83,4,76 >$. لتشفير الرسالة $\widehat{m} = 011101$ فأنها تحوّل الى العدد الصحيح 29 ومن ثم تجمع مع 1 للحصول على $\bar{m} = 30$. تربيع هذا العدد يعطي $m = 30^2 \bmod 167 = 65 \leq q$.

لنفترض اختيار $y = 71$ لغرض التشفير ، بالتالي نحصل على النص المشفر:

$$< [4^{71} \bmod 167], [67^{71}.65 \bmod 167] =< 132,44 >$$

لفك الشفرة ، يقوم المستلم اولا بحساب $[132^{37} \bmod 167] = 124$ وبما ان $[124^{-1} \bmod 167] = 66$ ، فإن المستلم يستطيع استرجاع الرسالة $m = 65 = [44.66 \bmod 167]$. هذه القيمة لها جذران اوليّان هما 30 و 137 ، ولكن الاخير اكبر من q. بذلك فإن $\bar{m} = 30$ والنص الاصلي يحسب بسهولة.

6.5.2 أمنية منهج El Gamal

تعتمد أمنية El Gamal بالدرجة الاساس على صعوبة حل مسألة اللوغاريتم المتقطع وبالتالي صعوبة معرفة x من $g^x \bmod q$ وهذا يتطلب ان تكون قيمة q على الاقل 300 مرتبة ، اضافة الى كون q عدد اولي ، كما ذكرنا في المقطع السابق.

- لاتقتصر أمنية منهج El Gamal على صعوبة مسألة اللوغاريتم المتقطع بل تعتمد على صعوبة مسألة DDH والتي تعني ان g^x لا يمكن تمييزه عن عدد عشوائي.
- على الرغم من مقاومة منهج El Gamal لمهاجمة CPA الّا انه لايصمد بوجه مهاجمة CCA كما هو حال منهج RSA.
- ولتوضيح ذلك ، افترض النص المشفر

$$< c_1, c_2 >=< g^y, h^y.m >.$$

يقوم الخصم بحساب $c'_2 = c_2.m'$. يمكن ببساطة اثبات ان فك شفرة النص الجديد $< c_1, c'_2 >$ هي $m.m'$.