مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (30) العدد (3) 2008
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (30) No. (2) 2008

دراسة مقارنة لدرجة سرية برامج مشاركة السرية

الدكتور تاج الدين جركس*
الدكتور عدنان معترماوي**
هنادي زهيرة***

(تاريخ الإيداع 29 / 1 / 2008. قُبِل للنشر في 2008/5/19)

□ الملخّص □

مع نهاية القرن العشرين تزايدت عمليات سرقة المصارف بالرغم من وجود كلمات مرور لحماية الحسابات، والسبب في ذلك يعود إلى قيام أحد عملاء المصرف المؤتمنين بتقديم كلمة السر(المفتاح السري) للمصرف إلى المختلسين . قاد هذا الأمر إلى إيجاد ما يسمى ببرنامج مشاركة السرية (Secret Sharing Scheme) لتحسين درجة السرية والأمان، وهو برنامج يتم فيه استخدام عدد من المشاركين؛ إذ يأخذ كل مُشارك جزءاً من المعلومات السرية ، التي لا يتمكن أي مشارك بمفرده من كشفها.

يهدف هذا البحث إلى دراسة مقارنة لدرجة سرية برامج مشاركة السرية، التي درست من قبل.

وفي نهاية البحث تم التوصل إلى النتائج التالية :

1- الأفضل برامج مشاركة السرية من أجل بنى وصول منتظمة.

2- اقتراح برنامج يهدف إلى تحسين الأمان، وحماية المعلومات السرية.

3- العلاقة بين درجة بنية الوصول وعدد المشاركين في كل مجموعة فرعية مفوضة

الكلمات المفتاحية : الأمان – السرية التامة (Perfect Secret) – برنامج مشاركة السرية – بنية الوصول (Access Structure) – المشاركة (Share) – المشارك (Participant) – برنامج العتبة (Threshold Scheme) .

* أستاذ – قسم هندسة الاتصالات والإلكترونيات – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين- اللاذقية – سورية .
** مدرس – قسم هندسة الاتصالات والإلكترونيات – كلية الهندسة الميكانيكية والكهربائية– جامعة تشرين- اللاذقية– سورية .
***طالبة دراسات عليا (ماجستير) – قسم هندسة الاتصالات والإلكترونيات – كلية الهندسة الميكانيكية والكهربائية– جامعة تشرين- اللاذقية – سورية .

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (30) العدد (3) 2008
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (30) No. (2) 2008

A Comparative Study of Secrecy Degree of Secret Sharing Schemes

Dr. Tajedin Jarkas*
Dr. Adnan Matarmawi**
Hanadi Zherah***

(Received 29 / 1 / 2008. Accepted 19 / 5 / 2008)

□ ABSTRACT □

Despite the use of passwords to protect computations, bank robbery has increased by the end of the twentieth century. This occurs when one of the bank employees passes the password to embezzlers. This matter has led to finding a secret sharing scheme to improve the security and secrecy degree; this scheme uses a number of participants, and each participant obtains a part of the secret information, whereupon none of the participants can unilaterally divulge this information. The research studies the secrecy degree of the Secret Sharing Schemes. Finally, we have highlighted the following:

1- The secret sharing schemes for uniform access structures is the best.

2- A scheme to improve the security and protection of secret information.

3- The relationship between the access structure degree and the number of participants in each secret sharing sub-group

Keywords: security- perfect secret. Secret sharing scheme(SSS) -Access structure-share-participant-threshold scheme.

***Professor, Department of communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.**
****Assistant Professor, Department of communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.**
*****Postgraduate student, Department of communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.**

مقدمة:

برنامج مشاركة السرية هو طريقة لمشاركة مفتاح السرية k بين مجموعة محدودة من المشاركين ، وهو برنامج مشاركة السرية يأخذ بعين الاعتبار السرية k الموزعة بين مجموعة من المشاركين إذ تتمكن مجموعات فرعية مؤهلة (مفوضة) من المشاركين من استرداد السرية ، بينما لا تتمكن المجموعات الفرعية غير المفوضة من المشاركين من الحصول على أية معلومة عن السرية .

انطلقنا في هذا البحث من نوع خاص من برامج مشاركة السرية يدعى برنامج العتبة ، من أجل بنى وصول منتظمة ، وبنى وصول غير منتظمة .

من خلال بحثنا نقارن بين برامج مشاركة السرية مع بنى وصول منتظمة ، و برامج مشاركة السرية مع بنى وصول غير منتظمة، من حيث السرية التامة، ومستوى الأمان والوثوقية ، كما سنقدم في نهاية البحث اقتراحاً عن العلاقة بين عدد المشاركين وعدد الأجزاء السرية ، بالإضافة إلى اقتراحات واستنتاجات أخرى .

أهمية البحث وأهدافه:

تكمن أهمية البحث المقدم في أنه يفتح آفاقاً جديدة لبناء برامج مشاركة سرية تامة غير قابلة للكسر، وتتماشى مع التطورات الهائلة في مجال التكنولوجيا وتطور نظرية المعلومات .

وتتلخص أهداف البحث في إبراز المشاكل التي تعاني منها برامج مشاركة السرية غير التامة، وكيفية التغلب عليها بجعل السرية تامة والوثوقية عالية، كما أننا سنقدم اقتراحاً عن العلاقة بين عدد المشاركين وعدد الأجزاء السرية التي لم تتناولها [7],[6],[5],[4],[3],[2],[1] ،وسنقترح برنامج مشاركة سرية لزيادة مستوى الأمان والوثوقية ، بالإضافة إلى اقتراحات واستنتاجات أخرى .

طريقة البحث ومواده:

يبدأ البحث بالتعرف على برامج العتبة، والمفاهيم المتعلقة بها مثل مفهوم بنية الوصول ومفهوم السرية التامة، ثم ينتقل إلى دراسة برامج مشاركة سرية من أجل بنى وصول منتظمة وغير منتظمة حيث ستتم دراسة :

1- برامج مشاركة سرية من أجل بنى وصول منتظمة مؤسسة علىGraph من درجة ثانية.

2- برامج مشاركة سرية من أجل بنى وصول منتظمة مؤسسة علىGraph من درجة رابعة.

3- برامج مشاركة سرية من أجل بنى وصول غير منتظمة .

ثم البحث عن العلاقة بين عدد الأجزاء السرية وعدد المشاركين من أجل بنى وصول منتظمة، ومن ثم تقديم البرنامج الذي سيتم اقتراحه في هذا البحث .

وأخيراً الاستنتاجات والتوصيات بالإضافة إلى قائمة بأسماء المراجع التي يستند إليها البحث .

مفهوم برنامج العتبة :

هو الطريقة لمشاركة المفتاح K بين مجموعة من n مشارك (يشار إليها عبر P)في هذه الطريقة إن أيّ t مشارك من أصل n مشارك يمكنهم حساب القيمة للسرية K ؛ إذ يكون الـ t مشاركاً ضمن بنية وصول ،لكن ليس

لأيّة مجموعة من $t-1$ مشارك أن تقوم بذلك ، لتكن t و n أعداداً صحيحة موجبة ، يرمز لبرنامج العتبة بالرمز $A(t,n)$.[1].

حيث n : العدد الكلي للمشاركين .

t : العدد الأصغري للمشاركين الذين يمكنهم استرداد السرية .

مثال على ذلك : برنامج العتبة $A(3,5)$ ، حيث $n=5$ ، $t=3$.

تملك برامج العتبة تطبيقات عديدة في مختلف المؤسسات ،مثل إطلاق الأسلحة النووية؛ إذ يكفي وجود ثلاثة مشاركين (وزير الدفاع ، وزارة الدفاع ، الرئيس) لإطلاق السلاح النووي من أصل خمسة مشاركين، بينما عندما يتواجد مشاركان اثنان فقط فإنهما لا يستطيعان إطلاق السلاح ، وبالتالي تكون السرية التامة محققة نوعاً ما .

إن مثل هذه البرامج تطبق في المصارف على المنوال نفسه.

مفهوم بنية الوصول :

سنستخدم مجموعة الرموز التالية:

$P=\left\{ p_i \quad ;1\le i\le n \right\}$ هي المجموعة من المشاركين .

الموزع (هو العنصر الأساسي المسؤول عن توزيع المشاركات على المشاركين)، ونرمز له بـ D ، ونفترض $D\notin P$.

K هي مجموعة المفتاح (المجموعة من جميع المفاتيح الممكنة) .

S هي مجموعة المشاركة (المجموعة من جميع المشاركات الممكنة) .

لتكن Γ مكونة من المجموعات الفرعية .

المجموعات الفرعية في Γ هي تلك المجموعات الفرعية من المشاركين الذين يجب أن يكونوا قادرين على حساب المفتاح (المعلومات السرية)، إذاً يدعى تجميع المجموعات الفرعية من المشاركين التي يمكنها إعادة حساب المفتاح (بناء السرية) بنية الوصول .[2].

حيث X : هي مجموعة فرعية من مجموعة المشاركين الأساسية .

ويمكن أن نعبر عن ذلك رياضياً :

$$\Gamma=\{X : X\in P\}$$

المجموعة من المجموعات الفرعية المؤهلة (المفوضة) الأصغرية من Γ تدعى الأساس لـ Γ ، ويرمز لها بـ Γ_0 ، وتدعى الإقفال لـ Γ ويرمز لذلك بـ $\Gamma=CL(\Gamma_0)$.

وبالتالي لدينا العبارة الرياضية التالية :

$$\Gamma=\{Y\subseteq P : X\subseteq Y, X\in\Gamma_0\}$$

حيث Y: هي المجموعة الفرعية المؤهلة الأصغرية من المشاركين .

مثال :

$$P = \{p_1, p_2, p_3, p_4\}$$

نحصل على :

$$\Gamma_0 = \{\{p_1, p_2, p_4\}, \{p_1, p_3, p_4\}, \{p_2, p_3\}\}$$

$$\Gamma = \Gamma_0 \cup \quad \{\{p_1, p_2, p_3\}, \{p_2, p_3, p_4\}, \{p_1, p_2, p_3, p_4\}\}$$

استخدام تابع الأنتروبيا لتعريف السرية التامة :

لقد ذكرنا في المقدمة أنّ المجموعات الفرعية المؤهلة (المفوضة) من المشاركين فقط يمكنها استرداد السرية ، بينما المجموعات الفرعية غير المفوضة من المشاركين لا يمكنها الحصول على أية معلومة عن السرية .

وهو ما يعرف بالسرية التامة.[3]

من خلال دراستنا لنظرية المعلومات نجد أن كمية المعلومات في الرسالة M تعرف بأنتروبيا الرسالة $H(M)$.

واعتماداً على هذا التعريف نقول: إذا كان K متغيراً عشوائياً يستولي على مجموعة فرعية من القيم تبعاً للاحتمال الموزع $P(k)$ فإنّ، الأنتروبيا للاحتمال الموزع هذا حددت لتكون :

$$H(K) = -\sum_{i=1}^{n} p_i \log p_i \qquad ; \quad 1 \le i \le n$$

إذا القيم الممكنة لـ x هي x_i ، حيث $1 \le i \le n$ ، عندئذ نجد :

$$H(K) = -\sum_{i=1}^{n} p(x = x_i) \log_2 p(x = x_i)$$

بشكلٍ مشابه وبفرض أن x و k هي قيم عشوائية ، عندئذ نعطي الاحتمال الشرطي $p(k/x)$ ، ونحدد الأنتروبيا الشرطية :

$$H(K/X) = -\sum_{k} p(k/x) \log_2 p(k/x)$$

بتطبيق هذا المفهوم على بحثنا نجد :

K تمثل سعة السرية (المفتاح) .

X تمثل مجموعة فرعية من المشاركين .

$$H(K.X) = H(K) + H(K/X)$$
$$H(K/X) = H(K.X) - H(X)$$

وبالتالي تكون شروط السرية تامة :

$$\forall_{X\in\Gamma} \quad H(K/X)=0 \qquad (1)$$

$$\forall_{X\notin\Gamma} \quad H(K/X)=H(K) \qquad (2)$$

من الشرط الأول (1) نستنتج أن :

أيّة مجموعة فرعية مفوضة يمكنها إعادة بناء السرية .

من الشرط الثاني(2) نستنتج أن :

أيّة مجموعة فرعية غير مفوضة لا تملك أية معلومات حول السرية .

بناء برنامج مشاركة سرية تامة من أجل بنى وصول منتظمة Graph –based من درجة ثانية: [3]

بفرض أن P هي مجموعة المشاركين ، إذا كانت بنية الوصول تتألف من مجموعات عدد المشاركين في كلٍ منها متساوٍ ، وإذا كانت كل مجموعة فرعية مفوضة أصغرية تملك الأساس نفسه عندئذ تسمى بنية الوصول منتظمة.

توضيح1: إن درجة بنية الوصول Γ هي الأساس من المجموعة الفرعية المؤهلة الأصغرية (مثلاً لدينا البرنامج $A(t,n)$ ، بالتالي لدينا برنامج من الدرجة t).

بنية وصول Graph –based يمكن أن تعد الحالة لبنية وصول من درجة ثانية (المرتبة لـ Γ اثنتين إذا كانت $\Gamma = CL(E(G))$).

توضيح 2: إذا $G=(V,E)$ هي Graph ، عندئذ نشير إلى مجموعة القمم لـ G عبر $V(G)$ ، ومجموعة الأضلع عبر $E(G)$ ،حيث كل قمة تمثل مشاركاً وكل ضلع يمثل الوصل بين زوج من المشاركين.

بنية الوصول Graph –based أسست على Graph يتألف من الرؤوس $V(G)$ والأضلع $E(G)$. بفرض G هي Graph مع الرؤوس $V(G)$ والأضلع $E(G)$ ، وبفرض أن $P=\{p_1,p_2,.....,p_n\}$ هي مجموعة من المشاركين (أي لدينا n قمة).

والسرية $K=(k_1,k_2)$ تؤخذ بشكل عشوائي من $GF(q^2)$ ،حيث q هو عدد أولي و $q\geq n$.

y_i تحسب من $f(x)$ كالتالي :

$$f(x)=k_2x+k_1 \bmod q$$

$$f(i-1) \bmod q = y_i \qquad ;i = 1,2,....n$$

الموزع يختار n رقماً عشوائياً $[r_1, r_2, ...r_n]$ من $GF(q)$.

المشاركة للمشارك p_i تعطى عبر :

$$S_i = \langle a_{i,1}, ..., a_{i,t}, ...a_{i,n} \rangle$$

حيث : $1 \le t \le n$

إذا $t = i \Leftarrow$ $a_{i,t} = r_i \bmod q$

إذا $\overline{p_i p_t}$ هي الحافة لـ $G \Leftarrow$ $a_{i,t} = r_t + y_t (\bmod q)$

إذا $t \ne i \Leftarrow$ و $\overline{p_i p_t}$ هي ليست الحافة لـ $G \Leftarrow$ $a_{i,t}$ فارغ .

هذا البرنامج يشبع شروط السرية التامة .

إذا تمكن شخص من الحصول على اثنين من y_i أو أكثر عندئذ يمكنه استرداد السرية .

إذا لم يتمكن هذا الشخص من الحصول على أيٍ من y_i فإنه لا يستطيع الحصول على أية معلومة حول السرية .

على سبيل المثال :

$P = \{p_1, p_2, p_3, p_4\}$ هي مجموعة من المشاركين .

وبفرض أن $q = 6 \ge n$.

$$\Gamma_0 = \{\{p_1, p_2\}, \{p_1, p_3\}, \{p_2, p_3\}, \{p_2, p_4\}\}$$

يختار الموزع n رقماً عشوائياً $(n = 4)$ $[r_1, r_2, r_3, r_4]$ من $GF(q)$.

والسرية : $K = (k_1, k_2) = (5,7)$

المشاركة للمشارك p_1 : $S_1 = \langle r_1, r_2 + y_2 \rangle$

المشاركة للمشارك p_2 : $S_2 = \langle r_2, r_3 + y_3 \rangle$

المشاركة للمشارك p_3 : $S_3 = \langle r_3, r_4 + y_4 \rangle$

المشاركة للمشارك p_4 : $S_4 = \langle r_4, r_1 + y_1 \rangle$

بناء برنامج مشاركة سرية تامة من أجل بنى وصول منتظمة من درجة رابعة:[3]

لتكن $P = \{p_1, p_2, ..., p_n\}$ هي مجموعة من المشاركين .

الخوارزمية التي يتم من خلالها مشاركة السرية بين مجموعة المشاركين هي التالية :

1- يتم حساب $m!$ (حيث m تمثل درجة بنية الوصول).

2- نختار عدداً أولياً q ، حيث $q \geq 2n$.

3- يتم تقسيم السرية إلى $m!$ جزء سري($k_1, k_2, k_3, ...k_{m!}$) ، تؤخذ هذه الأجزاء بشكل عشوائي من $GF(q^{m!})$.

4- نعين كثير حدود من درجة $m!-1$ ، أمثال كثير الحدود هي الأجزاء السرية :

$$f(x) = k_{m!}\ x^{m!-1} + k_{m!-1}\ x^{m!-2} + ... + k_3\ x^2 + k_2\ x\ + k_1 (\mathrm{mod}\, q)$$

y_i تحسب من $f(x)$ كالتالي :

$$y_i = f(i-1) \bmod\ \ q$$

5- نحدد G_i ، من أجل $1 \leq i \leq n$ ، كال Graph مع القمم $V(G_i)$ والحواف $E(G_i)$ كالتالي :

- $V(G_i)$ هي مجموعة القمم وهي تضم جميع المشاركين ماعدا المشارك p_i أي :

$$V(G_i) = \{p_j \,|\, for\ all\ \ p_j \in P\ /\{p_i\}\}$$

- $E(G_i)$ هي مجموعة تضم جميع الأضلع التي تصل بين القمم $V(G_i)$ أي :

$$E(G_i) = \{p_j p_k \,|\, for\ all\ \ p_j, p_k \in V(G_i)\}$$

6- نختار $2n$ رقماً عشوائياً $[r_1, r_2, ...r_{2n}]$ من $GF(q^{m!})$ ، ونقوم بتوزيعها على المشاركين بشكل سري، بحيث يحصل كل مشارك p_i على (r_i, r_{n+i}) .

7- يعطي الموزع المشاركة $a_{i,t}$ للمشارك p_i ، وبالتاي يحصل المشارك p_i على المشاركة:

$$S_i = \langle r_i, r_{i,n}, a_{i,1}, ..., a_{i,t}, ...a_{i,n} \rangle$$

حيث :

A. $a_{i,t} = S_i(G_t)$ If $p_i \in V(G_t)$

B. $a_{i,t} = r_t + y_t, r_{n+t} + y_{n+t}$ If $p_i p_t \in E(G\ )$

C. وبالحالات الأخرى $a_{i,t}$ فارغة .

الآن :

بفرض أننا نملك مجموعة المشاركين التالية : $P = \{p_1, p_2, ..., p_{14}\}$

وبنية الوصول منتظمة من درجة رابعة :

$$\Gamma_0 = \left\{ \begin{array}{l} \{p_1, p_2, p_3, p_4, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}\}, \\ \{p_2, p_3, p_4, p_5, p_6, p_7, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}\}, \\ \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{11}, p_{13}, p_{14}\}, \\ \{p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}\}, \\ \{p_1, p_3, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}\} \end{array} \right\}$$

بتنفيذ الخوارزمية:

1- $m = 4$ وبالتالي $m! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$.

2- $n = 14$ وبالتالي $q \geq 28$.

3- السرية $K = (k_1, k_2, k_3, ...k_{24})$ تؤخذ بشكل عشوائي من $GF(q^{24})$.

4- نعين كثير الحدود :

$$f(x) = k_{24}\, x^{23} + k_{23}\, x^{22} + ... + k_3\, x^2 + k_2\, x + k_1 (\mathrm{mod}\, q)$$

5- نحدد G_i من أجل $1 \leq i \leq 14$:

نبني G_1 مع :

$$V(G_1) = \{p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}\},$$
$$E(G_1) = \{\overline{p_2 p_3}, \overline{p_3 p_4}, \overline{p_4 p_5}, \overline{p_5 p_6}, \overline{p_6 p_7}, \overline{p_7 p_8}, \overline{p_8 p_9},$$
$$\overline{p_9 p_{10}}, \overline{p_{10} p_{11}}, \overline{p_{11} p_{12}}, \overline{p_{12} p_{13}}, \overline{p_{13} p_{14}}\}$$

نبني G_2 مع :

$$V(G_2) = \{p_1, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}\},$$
$$E(G_2) = \{\overline{p_1 p_3}, \overline{p_3 p_4}, \overline{p_4 p_6}, \overline{p_5 p_6}, \overline{p_5 p_7}, \overline{p_7 p_8}, \overline{p_1 p_9}, \overline{p_9 p_{11}},$$
$$\overline{p_{10} p_{11}}, \overline{p_{10} p_{12}}, \overline{p_{12} p_{13}}, \overline{p_{13} p_{14}}\}$$

نبني G_3 مع

$$V(G_3)=\{p_1,p_2,p_4,p_5,p_6,p_7,p_8,p_9,p_{10},p_{11},p_{12},p_{13},p_{14}\},$$
$$E(G_3)=\{\overline{p_1p_2},\overline{p_2p_5},\overline{p_4p_5},\overline{p_4p_6},\overline{p_6p_7},\overline{p_7p_9},\overline{p_8p_9},\overline{p_8p_{10}},$$
$$\overline{p_{10}p_{11}},\overline{p_{11}p_{14}},\overline{p_{12}p_{14}},\overline{p_{12}p_{13}}\}$$
$$V(G_4)=\{p_1,p_2,p_3,p_5,p_6,p_7,p_8,p_9,p_{10},p_{11},p_{12},p_{13},p_{14}\},$$
$$E(G_4)=\{\overline{p_1p_2},\overline{p_1p_3},\overline{p_3p_5},\overline{p_5p_6},\overline{p_6p_7},\overline{p_7p_9},\overline{p_8p_9},\overline{p_8p_{10}},$$
$$\overline{p_{10}p_{13}},\overline{p_{11}p_{13}},\overline{p_{11}p_{14}},\overline{p_{12}p_{13}}\}$$
$$V(G_5)=\{p_1,p_2,p_3,p_4,p_6,p_7,p_8,p_9,p_{10},p_{11},p_{12},p_{13},p_{14}\},$$
$$E(G_5)=\{\overline{p_1p_2},\overline{p_1p_3},\overline{p_3p_4},\overline{p_4p_6},\overline{p_6p_7},\overline{p_7p_9},\overline{p_8p_9},\overline{p_8p_{10}},$$
$$\overline{p_{10}p_{13}},\overline{p_{11}p_{13}},\overline{p_{11}p_{14}},\overline{p_{12}p_{13}}\}$$
$$V(G_6)=\{p_1,p_2,p_3,p_4,p_6,p_7,p_8,p_9,p_{10},p_{11},p_{12},p_{13},p_{14}\},$$
$$E(G_6)=\{\overline{p_1p_2},\overline{p_1p_3},\overline{p_3p_5},\overline{p_2p_4},\overline{p_4p_7},\overline{p_7p_9},\overline{p_8p_9},\overline{p_8p_{12}},$$
$$\overline{p_{10}p_{12}},\overline{p_{10}p_{11}},\overline{p_{11}p_{14}},\overline{p_{13}p_{14}}\}$$

وبهذه الطريقة نتابع بناء G_7 و G_8 و G_9 و G_{10} و G_{11} و G_{12} و G_{13} و G_{14} .

6- نختار 28 رقماً عشوائياً $[r_1,r_2,.....r_{28}]$ من $GF(q^{24})$.

7- كل زوج من $(r_i+y_i,r_{n+i}+y_{n+i})$ مشارك عبر برنامج مشاركة السرية مع بنية الوصول G_i.

المشاركة للمشارك p_i تعطى عبر :

$$S_1=\left\langle \begin{matrix} r_1,r_{15},-,S_1(G_2),S_1(G_3),S_1(G_4),S_1(G_5),S_1(G_6),S_1(G_7), \\ S_1(G_8),S_1(G_9),S_1(G_{10}),S_1(G_{11}),S_1(G_{12}),S_1(G_{13}),S_1(G_{14}) \end{matrix} \right\rangle$$

$$S_2=\left\langle \begin{matrix} r_2,r_{16},,S_2(G_1),-,S_2(G_3),S_2(G_4),S_2(G_5),S_2(G_6),S_2(G_7), \\ S_2(G_8),S_2(G_9),S_2(G_{10}),S_2(G_{11}),S_2(G_{12}),S_2(G_{13}),S_2(G_{14}) \end{matrix} \right\rangle$$

$$S_3 = \left\langle \begin{matrix} r_3, r_{17}, S_3(G_1), S_3(G_2), -, S_3(G_4), S_3(G_5), S_3(G_6), S_3(G_7), \\ S_3(G_8), S_3(G_9), S_3(G_{10}), S_3(G_{11}), S_3(G_{12}), S_3(G_{13}), S_3(G_{14}) \end{matrix} \right\rangle$$

$$S_4 = \left\langle \begin{matrix} r_4, r_{18}, S_4(G_1), S_4(G_2), S_4(G_3), -, S_4(G_5), S_4(G_6), S_4(G_7), \\ S_4(G_8), S_4(G_9), S_4(G_{10}), S_4(G_{11}), S_4(G_{12}), S_4(G_{13}), S_4(G_{14}) \end{matrix} \right\rangle$$

$$S_5 = \left\langle \begin{matrix} r_5, r_{19}, S_5(G_1), S_5(G_2), S_5(G_3), S_5(G_4), -, S_5(G_6), S_5(G_7), \\ S_5(G_8), S_5(G_9), S_5(G_{10}), S_5(G_{11}), S_5(G_{12}), S_5(G_{13}), S_5(G_{14}) \end{matrix} \right\rangle$$

$$S_6 = \left\langle \begin{matrix} r_6, r_{20}, S_6(G_1), S_6(G_2), S_6(G_3), S_6(G_4), S_6(G_5), -, S_6(G_7), \\ S_6(G_8), S_6(G_9), S_6(G_{10}), S_6(G_{11}), S_6(G_{12}), S_6(G_{13}), S_6(G_{14}) \end{matrix} \right\rangle$$

$$S_7 = \left\langle \begin{matrix} r_7, r_{21}, S_7(G_1), S_7(G_2), S_7(G_3), S_7(G_4), S_7(G_5), S_7(G_6), -, \\ S_7(G_8), S_7(G_9), S_7(G_{10}), S_7(G_{11}), S_7(G_{12}), S_7(G_{13}), S_7(G_{14}) \end{matrix} \right\rangle$$

$$S_8 = \left\langle \begin{matrix} r_8, r_{22}, S_8(G_1), S_8(G_2), S_8(G_3), S_8(G_4), S_8(G_5), S_8(G_6), \\ S_8(G_7), -, S_8(G_9), S_8(G_{10}), S_8(G_{11}), S_8(G_{12}), S_8(G_{13}), S_8(G_{14}) \end{matrix} \right\rangle$$

$$S_9 = \left\langle \begin{matrix} r_9, r_{23}, S_9(G_1), S_9(G_2), S_9(G_3), S_9(G_4), S_9(G_5), S_9(G_6), \\ S_9(G_7), S_9(G_8), -, S_9(G_{10}), S_9(G_{11}), S_9(G_{12}), S_9(G_{13}), S_9(G_{14}) \end{matrix} \right\rangle$$

$$S_{10} = \left\langle \begin{matrix} r_{10}, r_{24}, S_{10}(G_1), S_{10}(G_2), S_{10}(G_3), S_{10}(G_4), S_{10}(G_5), S_{10}(G_6), \\ S_{10}(G_7), S_{10}(G_8), S_{10}(G_9), -, S_{10}(G_{11}), S_{10}(G_{12}), S_{10}(G_{13}), S_{10}(G_{14}) \end{matrix} \right\rangle$$

$$S_{11} = \left\langle \begin{matrix} r_{11}, r_{25}, S_{11}(G_1), S_{11}(G_2), S_{11}(G_3), S_{11}(G_4), S_{11}(G_5), S_{11}(G_6), \\ S_{11}(G_7), S_{11}(G_8), S_{11}(G_9), S_{11}(G_{10}), -, S_{11}(G_{12}), S_{11}(G_{13}), S_{11}(G_{14}) \end{matrix} \right\rangle$$

$$S_{12} = \left\langle \begin{matrix} r_{12}, r_{26}, S_{12}(G_1), S_{12}(G_2), S_{12}(G_3), S_{12}(G_4), S_{12}(G_5), S_{12}(G_6), \\ S_{12}(G_7), S_{12}(G_8), S_{12}(G_9), S_{12}(G_{10}), S_{12}(G_{11}), -, S_{12}(G_{13}), S_{12}(G_{14}) \end{matrix} \right\rangle$$

$$S_{13} = \left\langle \begin{matrix} r_{13}, r_{27}, S_{13}(G_1), S_{13}(G_2), S_{13}(G_3), S_{13}(G_4), S_{13}(G_5), S_{13}(G_6), \\ S_{13}(G_7), S_{13}(G_8), S_{13}(G_9), S_{13}(G_{10}), S_{13}(G_{11}), S_{13}(G_{12}), -, S_{13}(G_{14}) \end{matrix} \right\rangle$$

$$S_{14}=\left\langle \begin{matrix} r_{14}, r_{28}, S_{14}(G_1), S_{14}(G_2), S_{14}(G_3), S_{14}(G_4), S_{14}(G_5), S_{14}(G_6), \\ S_{14}(G_7), S_{14}(G_8), S_{14}(G_9), S_{14}(G_{10}), S_{14}(G_{11}), S_{14}(G_{12}), S_{14}(G_{13}), - \end{matrix} \right\rangle$$

بالنسبة للمجموعة الفرعية المؤهلة التالية :

$$B=\{p_2, p_3, p_4, p_5, p_6, p_7, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}\}$$

(مثلاً $\overline{p_2 p_3}$ هو ضلع ينتمي لـ $E(G_1)$ وبالتالي من $S_2(G_1)$ و $S_3(G_1)$ يمكن أن نسترد $(r_1+y_1, r_{15}+y_{15})$ وهكذا) .

بالتعويض في y_i نجد أننا نحصل على أربع وعشرين قيمة لـ K وبالتالي يمكننا الحصول على السرية (المعلومات السرية)كاملة .

برنامج مشاركة سرية تامة من أجل بنى وصول غير منتظمة:

بفرض أن $P=\{p_1, p_2, \ldots\ldots, p_n\}$ هي مجموعة المشاركين ، إن بنية الوصول تدعى غير منتظمة إذا كان لكلّ مجموعة فرعية مفوضة أصغرية أساس مختلف .

بالتالي إذا كانت بنية الوصول مؤلفة من مجموعات عدد المشاركين في كلٍ منها يختلف عن الأخرى، تسمى بنية الوصول غير منتظمة .

الشيء الجديد في هذا البرنامج هو أن المشاركين متفاوتون في درجة الأهمية ، وبالتالي سيكون مشارك أهم من مشارك آخر،بمعنى آخر سيتواجد هناك مشارك يملك حصص(أجزاء) أكثر من المشاركين الآخرين ، فمثلاً المجموعة الفرعية المفوضة التي تحتوي على مشارِكين فقط ، لكي تتمكن من إعادة بناء السرية يجب أن تملك جميع الأجزاء، إذاً كل مشارك من هذين المشاركين يملك أكثر من حصة. وبالتالي كل مشارك يختلف بالأهمية وذلك حسب الأجزاء التي يملكها .

مثلاً لتكن لدينا مجموعة المشاركين:

$$P=\{p_1, p_2, p_3, p_4\}$$

وبنية الوصول هي :

$$\Gamma_0=\{\{p_1, p_2\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$$

من بنية الوصول هذه نجد أن المشارِكين p_1 و p_2 سيُعطى لكلٍ منهما نصف الأجزاء السرية ، وبالتالي فإن المشارِكين p_3 و p_4 كلاهما يكافئان أحد المشارِكين إما المشارك p_1 وإما المشارك p_2 من حيث كمية المعلومات التي يحملانها عن السرية .

وبالتالي لا توجد قاعدة معينة لتوزيع السرية ، كما أن احتمال السرية التامة سيكون أقل؛ لأنه إذا أخذنا المجموعة الفرعية غير المفوضة $D=\{p_1, p_2, p_3\}$

نجد أنها قادرة على كشف السرية.

وبالتالي فإن هذا يتطلّب مجهوداً أكبر ودقة أكثر في توزيع الأجزاء السرية ، بحيث لا تتمكن أية مجموعة غير مفوضة من كشف السرية .

العلاقة التي سيتم اقتراحها في هذا البحث بين عدد الأجزاء السرية وعدد المشاركين في كل مجموعة فرعية مفوضة من أجل بنى وصول منتظمة هي:

لتكن $P = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ مع بنى وصول منتظمة من درجة رابعة .

وبنية الوصول :

$$\Gamma_0 = \left\{ \begin{matrix} \{p_1, p_2, p_3, p_4\}, \{p_2, p_4, p_5, p_6\}, \{p_1, p_3, p_5, p_6\}, \\ p_2, p_3, p_4, p_6\}, \{p_1, p_2, p_4, p_6\}, \{p_3, p_4, p_5, p_6\} \end{matrix} \right\}$$

أي $n = 6$

السرية : $K = (k_1, k_2, k_3, \ldots\ldots k_{24})$

تؤخذ بشكل عشوائي من $GF(q^{24})$ ، حيث q هو عدد أولي و $q \geq 12$.

ليكن :

$$f(x) = k_{24}\, x^{23} + k_{23}\, x^{22} + \ldots\ldots\ldots + k_3\, x^2 + k_2\, x + k_1 (\mathrm{mod}\, q)$$

y_i تحسب من $f(x)$ كالتالي :

$$y_i = f(i-1) \bmod q \qquad ; i = 1,2,\ldots.12$$

نحدد G_i من أجل $1 \leq i \leq n$ ، كالـ Graph مع القمم $V(G_i)$ والحواف $E(G_i)$.

نبني G_1 مع :

$$V(G_1) = \{p_2, p_3, p_4, p_5, p_6\}, E(G_1) = \{\overline{p_2 p_3}, \overline{p_2 p_4}, \overline{p_3 p_5}, \overline{p_5 p_6}\}$$

نبني G_2 مع :

$$V(G_2) = \{p_1, p_3, p_4, p_5, p_6\}, E(G_2) = \{\overline{p_1 p_3}, \overline{p_1 p_4}, \overline{p_4 p_5}, \overline{p_5 p_6}\}$$

نبني G_3 مع :

$$V(G_3) = \{p_1, p_2, p_4, p_5, p_6\}, E(G_3) = \{\overline{p_1 p_2}, \overline{p_2 p_4}, \overline{p_4 p_5}, \overline{p_1 p_6}\}$$

نبني G_4 مع :

$$V(G_4) = \{p_1, p_2, p_3, p_5, p_6\}, E(G_4) = \{\overline{p_1 p_2}, \overline{p_2 p_3}, \overline{p_3 p_5}, \overline{p_5 p_6}\}$$

نبني G_5 مع :

$$V(G_5)=\{p_1, p_2, p_3, p_4, p_6\}, E(G_5)=\{\overline{p_1p_3}, \overline{p_3p_4}, \overline{p_2p_4}, \overline{p_1p_6}\}$$

نبني G_6 مع :

$$V(G_6)=\{p_1, p_2, p_3, p_4, p_5\}, E(G_6)=\{\overline{p_1p_2}, \overline{p_2p_3}, \overline{p_3p_4}, \overline{p_4p_5}\}$$

يختار الموزع 12 رقماً عشوائياً $[r_1, r_2, \ldots\ldots r_{12}]$ من $GF(q^{24})$ ، كل زوج من $(r_i + y_i, r_{n+i} + y_{n+i})$ مشارك عبر برنامج المشاركة السرية مع بنية الوصول G_i ،

والمشاركة للمشارك p_j هي $S_j(G_i)$ من أجل $p_j \in V(G_i)$

المشاركة للمشارك p_i تعطى عبر :

$$S_1=\left\langle r_1, r_7, -, S_1(G_2), S_1(G_3), S_1(G_4), S_1(G_5), S_1(G_6)\right\rangle$$

$$S_2=\left\langle r_2, r_8, , S_2(G_1), -, S_2(G_3), S_2(G_4), S_2(G_5), S_2(G_6)\right\rangle$$

$$S_3=\left\langle r_3, r_9, S_3(G_1), S_3(G_2), -, S_3(G_4), S_3(G_5), S_3(G_6)\right\rangle$$

$$S_4=\left\langle r_4, r_{10}, S_4(G_1), S_4(G_2), S_4(G_3), -, S_4(G_5), S_4(G_6)\right\rangle$$

$$S_5=\left\langle r_5, r_{11}, S_5(G_1), S_5(G_2), S_5(G_3), S_5(G_4), -, S_5(G_6)\right\rangle$$

$$S_6=\left\langle r_6, r_{12}, S_6(G_1), S_6(G_2), S_6(G_3), S_6(G_4), S_6(G_5), -\right\rangle$$

بالنسبة إلى المجموعة الفرعية المؤهلة التالية : $B=\{p_1, p_2, p_3, p_4\}$

حيث $B \in \Gamma_0$ يمكن أن

تسترد $[y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12}]$

بالتعويض في y_i نجد أننا نحصل على اثنتي عشر قيمة لـ k ، وبالتالي لا يمكننا الحصول على السرية (المعلومات السرية)كاملة .

وبالتالي نستنتج أن عدد المشاركين في كل مجموعة فرعية مفوضة يجب أن يكون اثني عشر مشاركاً على الأقل لكي يتمكنوا من إعادة بناء السرية .

إذاً نتوصل إلى أن العلاقة بين عدد الأجزاء السرية ، وعدد المشاركين في كل مجموعة فرعية مفوضة هي:

$$t \geq l/2$$

حيث : l هو عدد أجزاء المفتاح السري .

أي أن عدد المشاركين يجب أن يؤخذ بحيث أن كل مجموعة فرعية مفوضة تحصل على جميع الأجزاء السرية مثلاً في المثال أعلاه $t = 4$ هو غير كافٍ للحصول على جميع الأجزاء .

إذاً ليس لأية مجموعة فرعية مفوضة أن تحصل على المفتاح السري (السرية كاملة) ، كما أن المجموعة P نفسها غير قادرة على الحصول على المفتاح السري (السرية كاملة) .

إذاً الموزع هو الوحيد الذي يعلم المفتاح وبالتالي لم تتحقق أية مشاركة بالسرية .

أعظم حالة لـ t هي t=n، وستكون بنية الوصول Γ هي نفسها P ، إذاً لن تتمكن هذه المجموعة من كشف السرية ، أي المعلومات التي تم توزيعها على المشاركين غير كاملة ، وسيبقى الموزع هو الوحيد الذي يعلم السرية، ولن يتم كشفها إلا من قبله .ولم يعد هناك ما يسمى ببرنامج مشاركة السرية.

برنامج مشاركة السرية الذي سنقترحه في هذا البحث:

لنفترض أن برنامج العتبة يقوم على أساس أن عدد المشاركات هو مساوٍ لـ t عدد المشاركين في كل مجموعة فرعية مفوضة ضمن بنية الوصول .

بشكلٍ أوضح يتم تقسيم السرية إلى t مشاركة ، كل مشاركة تعطى لمجموعة فرعية مفوضة محتواة في بنية الوصول .

بفرض $P = \{p_1, p_2, p_3, p_4\}$ هي مجموعة المشاركين .

وبنية الوصول هي $\Gamma_0 = \{\{p_1, p_2\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$

السرية ستقسم إلى ثلاث مشاركات؛ لأن عدد المجموعات الفرعية المفوضة ضمن بنية الوصول يساوي ثلاث مجموعات.

k_1 تعطى للمجموعة $\{p_1, p_2\}$

k_2 تعطى للمجموعة $\{p_1, p_3, p_4\}$

k_3 تعطى للمجموعة $\{p_2, p_3, p_4\}$

1- نقاط القوة والضعف للبرنامج المقترح :

نقاط القوة:

1-إن غياب أحد المشاركين لا يعني أبداً غياب جزء من السر. لأنه من الممكن الحصول على هذا الجزء من قبل مشارك آخر .

2- زيادة درجة السرية .

الثغرات التي سنتعرض لها في أثناء تطبيق هذا البرنامج(نقاط الضعف) هي :

- السرية غير تامة؛ لأن المجموعة الفرعية المفوضة $B=\{p_1, p_2\}$ ستكون قادرة على كشف السر من دون اللجوء إلى المجموعات الفرعية المفوضة الأخرى؛ لأن المشارك p_1 يعلم الحصص k_1 و k_2، والمشارك p_2 يعلم الحصص k_2 و k_3، إذاً هذه المجموعة قادرة على كشف السر .
- سيكون هناك مشارك يملك أكثر من حصة؛ لأنه موجود في أكثر من مجموعة ، وبالتالي هذا المشارك لوحده سيعلم السر، وبالتالي يكسر مفهوم السرية التامة ، كما أن مفهوم المشاركة بالسر (تجزئة المعلومات السرية) سيختفي ، وسنعود لمفهوم أحادية السر ، هنا مثلاً المشارك p_4 يعلم الحصة k_2 و k_3، والمشارك p_3 يعلم الحصة k_2 و k_3 ، إذاً ليس بالضرورة وجود هذه المجموعات أو اجتماعها للحصول على السرية .

2- *الحلول المقترحة لحل هذه الثغرات*:

- أن تكون بنى الوصول منتظمة .
- أن لا يتكرر وجود مشارك من المشاركين في أكثر من مجموعة .
- زيادة عدد المشاركين؛ لأن هذا الأمر يقود إلى زيادة درجة الأمان؛ أي احتمال كشف السرية ضئيل جداً جداً ، كما أنه إذا تم فقد الاتصال مع أحد المشاركين سيكون هناك مشارك آخر يقوم مكانه .

الشيء الجديد في هذا البرنامج هو أن درجة السرية والأمان ازدادت ، واحتمال كشف السرية أقل ، كما ازدادت وثوقية الشخص الذي يتعامل مع هذا البرنامج بالبرنامج .

3- *مثال على البرنامج المقترح* :

لتكن مجموعة المشاركين هي : $P=\{p_1, p_2, p_3, p_4, p_5, p_6\}$ و $q>n$

و بنية الوصول هي : $\Gamma_0=\{\{p_1, p_2\}, \{p_3, p_4\}, \{p_5, p_6\}\}$

والمفتاح السري سيقسم إلى ثلاث مشاركات؛ لأن عدد المجموعات الفرعية المفوضة ضمن بنية الوصول يساوي ثلاث مجموعات:

$$K=(k_1, k_2, k_3)=(9,3,1)$$

k_1 تعطى للمجموعة $\{p_1, p_2\}$

k_2 تعطى للمجموعة $\{p_3, p_4\}$

k_3 تعطى للمجموعة $\{p_5, p_6\}$

بفرض أن $q=11$ نحصل على

المشاركة للمشارك p_1 : $S_1=k_1'=12$ و المشاركة للمشارك p_2 : $S_2=k_1''=8$

المشاركة للمشارك p_3 : $S_3=k_2'=10$ و المشاركة للمشارك p_4 : $S_4=k_2''=4$

المشاركة للمشارك p_5 : $S_5=k_3'=16$ و المشاركة للمشارك p_6 : $S_6=k_3''=18$

حيث: $k_1=(k_1'+k_1'')\bmod q$

$k_2=(k_2'+k_2'')\bmod q$ ، $k_3=(k_3'+k_3'')\bmod q$

يجب أن يتم اختيار المشاركات k_1'' و k_1' و k_2'' و k_2' و k_3'' و k_3' بشكل دقيق، بحيث لا تتمكن أية مجموعة غير مفوضة من المشاركين من الحصول على السرية، على سبيل المثال إذا قام المشارك p_1 و المشارك p_5 ($\{p_1,p_5\}$ مجموعة غير مفوضة) بجمع مشاركتهما معاً فلن يتمكنا من الحصول على السرية K ؛ لأن $(12+16)\bmod 11=(28)\bmod 11=6$ وهو جزء سري خاطئ.

الاستنتاجات والتوصيات:

لقد تم التوصل في هذا البحث إلى الاستنتاجات التالية :

1- بإجراء مقارنة بين برنامج مشاركة سرية من درجة ثانية وبرنامج مشاركة سرية من درجة رابعة نجد أنه كلما زدنا درجة بنية الوصول كلما زاد احتمال السرية التامة؛ أي كلما قل احتمال كشف المعلومات والبيانات السرية؛ وذلك لأن السرية ستقسم إلى مشاركات أكثر، وبالتالي احتمال كشف السرية أقل . إذاً كلما كان عدد المشاركين أكثر كلما كانت درجة الآمان أفضل .

2- بإجراء مقارنة بين برنامج مشاركة سرية من أجل بنى وصول منتظمة وبرنامج مشاركة سرية من أجل بنى وصول غير منتظمة ، نجد أن احتمال السرية التامة سيكون أقل مع بنى وصول غير منتظمة، في حال لم يتم توزيع الأجزاء بدقة وعناية فائقة جداً ، إذاً برنامج مشاركة سرية من أجل بنى وصول منتظمة هو الأفضل والأقوى من ناحية السرية التامة ومستوى الأمان .

3- توصلنا إلى العلاقة التالية بين درجة بنية الوصول ، وعدد المشاركين في كل مجموعة فرعية مفوضة :

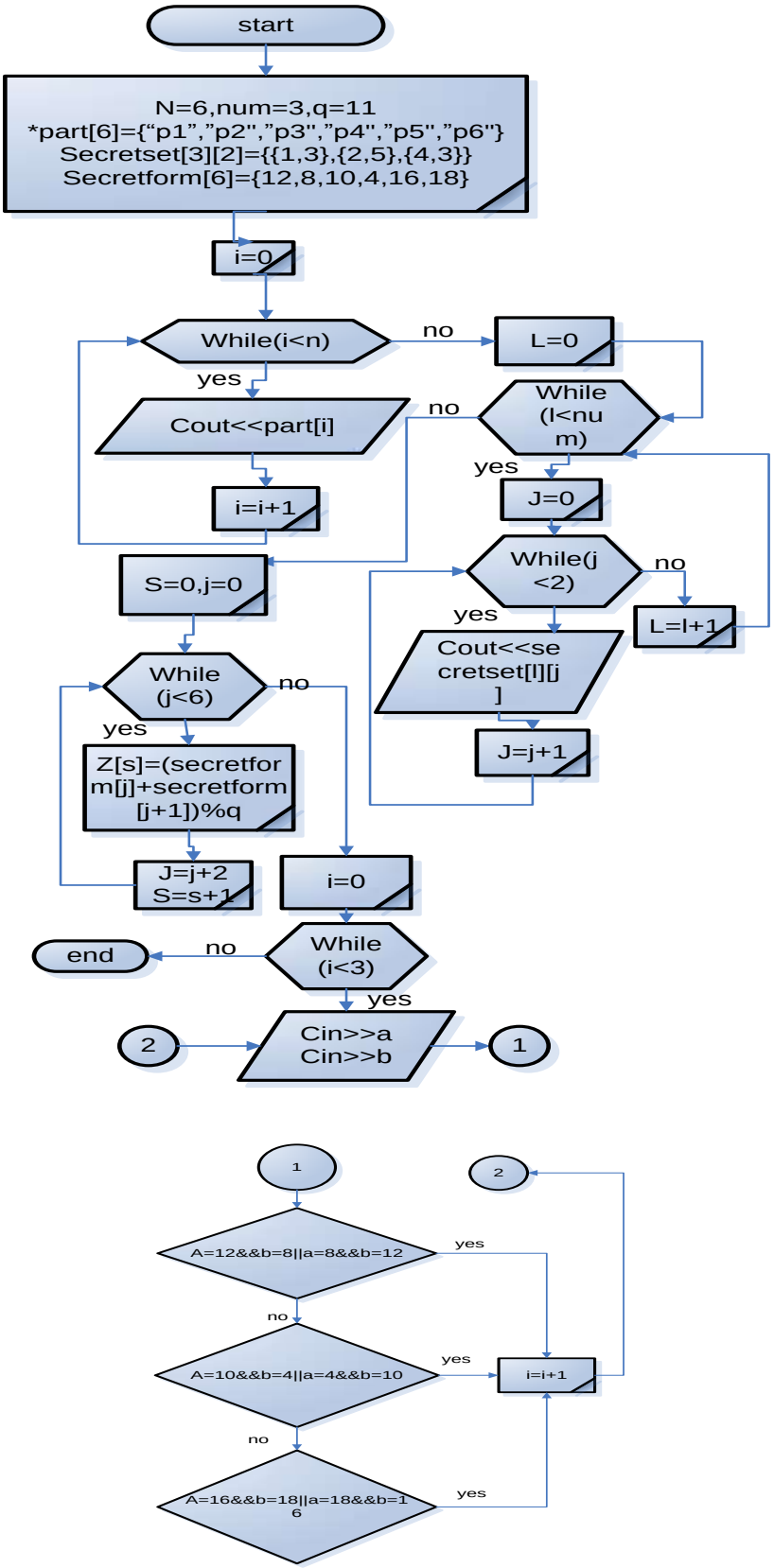
$$t\geq l/2$$

4- عدد العناصر في مجموعة المشاركين P يجب أن يؤخذ بعناية أو بمعنى آخر بدقة أكثر وليس عشوائياً؛ وذلك لزيادة درجة الأمان ، وزيادة احتمال السرية التامة ، ولتحقيق مبدأ المشاركة بالسرية .

كما تم بهدف زيادة مستوى الأمان والسرية التامة اقتراح :

1-البرنامج الذي بنيناه بالاعتماد على مبدأ تحسين الأمان وحماية المعلومات والبيانات السرية .

2-استخدام برامج مشاركة السرية مع بنى وصول منتظمة من درجة عالية .



الشكل (1) خوارزمية البرنامج المقترح لتحسين الأمان

المراجع:

1-DOUGLAS , R . S . *Cryptography – Theory and Practice* , Second Edition , CRC Press ,New Jersey , 2000,1-4o8.

2- D . R . Stinson , *Decomposition Construction for Secret Sharing Schemes,* IEEE Trans.Inform . Theory Vol 40 (1994)pp 118-125 .

3- SUN .Hung –Min ; Shien. Shiuh –Pyng , *Constructing Perfect Secret Sharing Schemes for General and Uniform Access Structucteres,*Journal of Information Science and Engineering 15 ,1999,pp679-689.

4- SHAMIR , A . *How to Share a Secret* , Communications of The ACM 22, 11,1979, pp 612- 613 .

5- STALLINGS ,W . *Cryptography and Network Security* , Principles and Practice Second Edition , Prentice Hall , New Jersey , 1999, 1-537 .

6- STALLINGS ,W . *Cryptography and Network Security* , Fourth Edition , United States of America, 2006, 1-656.

7- شنایر ، بروس ، النجدي ، حاتم ، الدكاك ، أميمة . *التعمية التطبيقية – موافيق وخوارزميات ورماز مصدري باللغة C* ، الطبعة الثانية – الجمعية العلمية السورية للمعلوماتية ، سورية,2006 ، 350-100 .

ملحق:

لقد تم برمجة البرنامج الذي تم اقتراحه في هذا البحث بالاعتماد على لغة البرمجة الـ C^{++}

```
# include<iostream.h>
#include<conion.h>
void main( )
{ int n=6,i;
   int a,b;
int z[3];
int j,q=11;
char *part[6]={"p1","p2","p3","p4","p5","p6"};
int secretset[3][2]={{1,3},{2,5},{4,6}};
int secretform[6]={12,8,10,4,16,18};
int num=3;
for(i=0;i<n;i++)
cout<<part[i]<<'  ';
cout<<endl<<endl;
cout<<"the secret sets are as the following:\n";
for(i=0;i<num;i++)
{
cout<<"the set is: ";
for(j=0;j<2;j++)
cout<<secretset[i][j]<<"  ";
cout<<endl;}
cout<<endl;
cout<<"where 1 means the participant p1 and 2 means p2 and so on…….\n";
int s=0;
j=0;
while(j<6)
{z[s]=((secretform[j]+secretform[j+1])%q);
j=j+2;
s++;}
cout<<"enter the right numbers to know right part of secret";
for(i=0;i<3;i++)
{cin>>a;
cout<<endl;
cin>>b;
if(((a==12)&&(b==8))||((a==8)&&(b==12)))
cout<<"this is the first number of the secret:"<<z[0];
else
If(((a==4)&&(b==10))||((a==10)&&(b==4)))
cout<<"this is the second number of the secret:"<<z[1];
else
if(((a==16)&&(b==18))||((a==18)&&(b==16)))
cout<<"this is the third number of the secret:"<<z[2];
else
cout<<"error in input, you will not has the secret";}
getch();}
```

ويكون تنفيذ البرنامج كالتالي: