حزمة برمجيات و مكتبة
EnDaBi
تشفير ، قواعد بيانات ، قياسات بيومترية

علي شمحل، رؤى سليمان، عالية سلمان، الياس سعود، مطيع رحمون، وسيم علي

بإشراف المهندس : سامي أبوبالا

٦ تشرين الثاني ٢٠١٥

الفهرس

الباب ١

فهرس الأشكال :

الباب ٢

فهرس الرماز المصدري :

١- *ENDABI RSA CORE*
٢- *ENDABI RSA DEMO*
٣- *ENDABI RSA DEMO GUI*
٤- *SEGMENTED SIEVE*
٥- *ISProbablePrime*
٦- *makefile*

الباب ٣

جدول المصطلحات :

RSA *Ron Rivest , Adi Shamir and Leonard Adlemn* ، **خوارزمية تشفير غير متناظر .**
MIT *Massachusetts Institute of Technology* ، **جامعة أميركية مرموقة تختص بعلوم الحاسب .**
Prerequisites **متطلبات التنزيل .**
Terminal **محرر الأوامر الخاص بأنظمة اليونكس .**

الباب ٤

توثيق (النسخة العربية) :

هذا التوثيق ، بالإضافة لتوثيق بلغات أخرى ، الرماز المصدري ، الرخص و
كل المواد المرتبطة بمشروع *EnDaBi* مسجلة و محتواة على :
https://github.com/EnDABi/EnDaBi

الباب ٥

الرخصة

١.٥ اشعار الرخصة

٢.٥ مجموعة رخص ال EnDaBi :

توثيقنا (كما هو موضح في السابق) مرخص تحت رخصة *GNU Free Documentation License* .
لكن رمازنا المصدري مرخص تحت رخصة
GNU Lesser General Public License

٣.٥ أمور قانونية:

هذا التوثيق هو دليل لحزمة من البرمجيّات المجانيّة مفتوحة المصدر ، التي هي بالإضافة إلى التوثيق ، تم وضعها من قبل فريق صغير من المهندسين الشبّاب كمشروع للسنة الثالثة في جامعة تشرين ، اللاذقية ، سوريا.

الشّيفرة تطبّق خوارزميّات حوسبيّة و رياضيّة معروفة و عموميّة ، مستخدمة لغات برمجة مجانية مفتوحة المصدر ، تم اختبارها و تنفيذها على منصّات مجانية مفتوحة المصدر باستخدام برمجيّات مجانية مفتوحة المصدر.
عملنا لا يتضمن أية برمجيات مغلقة المصدر أو ذات حقوق ملكيّة.
بعض من تطبيقاتنا المضمنة أصلي على أنه مختلف.
على كل حال ، الفكرة من المشروع ، و التّطبيقات الفرديّة للخوارزميّات و الصيغ الرياضيّة كلها عمومية.
ما يعني أنّه من الممكن أن يوجد تشابه كبير مع اعمال أخرى في العالم.
و في حال حدوث ذلك ، إذا ما كان التّشابه يمكن تفريقه فإننا على استعداد لإعادة تطبيقه ، و في حال حدوث ذلك يرجى التّواصل معنا على البريد الإلكتروني التالي
.aly.shmahell@gmail.com
و سيكون هناك حوار في أول فرصة تسمح لنا بقراءة البريد الإلكتروني و الرد عليه.
يرجى الملاحظة و الإنتباه إلى أنّ هذا لا يعني أنّنا سنكون عرضة للاستفزاز ، إذ إنّ أي محاولة لاستفزاز عملنا أو جرّنا إلى جدال غير قانوني لن يتم التسامح في خصوصها.

٤.٥ تصريح عن عدم المسؤوليّة:

إن هذه البرمجيّات متوفّرة كما هي ، دون أي ضمانات من أيّ نوع سواء أكانت صريحة أو ضمنيّة ، تشمل ولكنها غير محدّدة ب (ضمانات تجاريّة ، المناسبة لهدف محدد) .

و لا في أيّ حالٍ سيكون على المؤلّفين أو حاملي حقوق النّشر مسؤوليّة عن أيّ ادعاء أو أضرار أو أيّ مسؤوليّة أخرى،
سواء في حال إجراء عقود أو أي ضرر آخر من الأضرار النّاجمة من داخل البرمجيّات ، أو خارجها ، أو خلال الإتصال مع البرمجيّات ، أو خلال الاستخدام ، أو أية تعاملات أخرى في البرمجيات.
إنّ الاستخدام سيكون على مسؤوليّتك الخاصّة.
القصد من هذا المشروع هو خدمة الإنسان ، ومعالجة مشاكل الخصوصيّة و سهولة الوصول. و إنه من المتوقع أن يتمّ استخدامه بهذه الطّريقة.
نحن لسنا مذنبين أو مسؤولين عن أيّ سوء استخدام لمشروعنا.

الباب ٦

لمحة عن المؤلّفين:

نحن مواطنون سوريّون ، يعتبرون أنفسهم مواطنين لبلدهم و العالم على حدّ سواء.

وفيما يلي قائمة بالمؤلّفين و معلومات الإتّصال بهم:

الاسم	الإيميل
علي شمحل	*aly.shmahell@gmail.com*
الياس سعود	*Thegamebest21es@gmail.com*
عالية سلمان	*el57la.9595@gmail.com*
رؤى سليمان	*ruaa.s.sleiman@gmail.com*
مطيع رحمون	*Mrahmoon1994@gmail.com*
وسيم علي	*wali91350@gmail.com*

الباب ٧

شكر خاص :

نعطي شكرنا إلى كل من ساعدونا:
المشرف على مشروعنا المهندس : سامي أبوبالا .
الذي كان صبره و مساعدته لنا شيء حاسم و بالغ الأهمية في تقديم و نجاح عملنا الأول .
البروفيسور الدكتور المهندس : كريستوف بار
من جامعة روهر في بوخوم في ألمانيا .الذي بنينا هذا العمل على عمله و معلوماته ، و نشكره جزيل الشكر للطفه البالغ في السماح لنا بتضمين أجزاء من محاضراته في توثيقنا هذا

الباب ٨

المقدمة:

الأمان و الخصوصية جانب أساسي في حياتنا . لنأخذ على سبيل المثال رجل الكهف ، خيار الحياة له كان أن يستقر عن الصيد و الإلتقاط ،مما وفر له المزيد من الأمان داخل كهفه ، ولكن من جانب آخر فإن هذا حد من حريته في التجوال في الأراضي الشاسعة .
و نفس هذا الجانب يمكن أن نراه في المجتمعات الحديثة ، فلنأخذ شركة ما على سبيل المثال ، حيث أنها إذا ما خففت من معايير الأمان على مداخلها ، فإن ذلك سوف يسهل على الموظفين الدخول بشكل أسرع من جانب (لن يكونو بحاجة لإبراز الكثير من البطاقات للتعريف بأنفسهم أو تذكر العديد من كلمات المرور و غير ذلك..) ،
و لكن من جانب آخر فإن الشركة سوف تفقد بعضاْ من نقاط الأمان فيها ، والعكس صحيح.
مشروع $EnDaBi$ يحل هذه المشكلة ، و يحاول بأن يجد التوازن بين الأمان و الحركية ، و ذلك باستخدام أحدث الطرق في التشفير ، وقواعد البيانات ، وتقنيات القياسات البيومترية ، و دمجهم في مكتبة واحدة متماسكة فعالة لتحقيق الهدف.

الباب ٩

لمحة عن المشرروع:

وعد المشروع بسيط ، بداية ركزنا على التشفير و أمن المعلومات .
بحثنا طويلا عن مواد علمية مناسبة تخدم هذا الغرض المعين .
ووجدنا تلك التي وضعها رئيس قسم التشفير التطبيقي في منظمة
Intarnet of Things
البروفيسور كريستوف بار المدرس في جامعة *MIT* ،
الأنسب من أجل التطبيق العملي و الأكثر سهولة للفهم .

الباب ٠١

خطوات المشروع الحالية:

١- اختيار خوارزمية ال RSA كبداية ،سبب ذلك معايير الأمان القوية التي تحققها، و كذلك حرية الحركة التي تسمح بها و قابلية التطبيق الواسعة كونها تتبع لنمط التشفير غير المتناظر .

٢- محاولة تحقيق خوارزمية ال RSA بأكبر شكل بسيط و عملي .

٣- السعي لتطوير المكتبة من أجل تحسين الأداء و السرعة.

٤- السعي لنقل المكتبة إلى أكبر عدد من لغات البرمجة و المنصات الحوسبية.

الباب ١١

علم التشفير :

يتطرق هذا العلم إلى جعل المعلومات التي هي متوفرة أصلاً للعموم مقروءة أو مفهومة فقط لقلة مختارة.

يوجد العديد من التصنيفات لطرق التشفير و هي:

الباب ٢١

التشفير المتناظر:

هو تصنيف يتضمن تبادل مفتاح مشترك بين الأطراف المشاركة في التشفير.
⋆يستخدم هذا المفتاح من أجل التشفير و فك التشفير معاً.
⋆المفتاح يجب أن يتم تبادله على قناة آمنة و إلا سيكون من الممكن التقاطه من قبل شخص ثالث متنصت سيقوم باستخدامه من أجل فك تشفير المحادثة.

الباب ٣١

التشفير غير المتناظر:

هذا التصنيف من التشفير يتضمن زوج من المفاتيح (عمومي و خصوصي) .

* المفتاح العمومي يستخدم للتشفير فقط.
* المفتاح الخصوصي يستخدم لفك التشفير فقط.
* فقط المفتاح العمومي يتم تبادله على الشبكة.
* و على ذلك إذا تنصت شخص ثالث على التبادل فإنه لن يستطيع فك التشفير.

الباب ٤١

خلفية رياضية:

تستخدم خوارزمية ال RSA مجموعة من الطرائق و المعادلات الرياضية المعروفة لتحقيق تشفير و فك تشفير ناجح و آمن .

و هذه تتضمن :
١- الخوارزمية الإقليدية.
٢- الخوارزمية الإقليدية الممددة.
٣- تابع فاي لأويلر.
٤- نظرية فيرمات الصغيرة.
٥- نظرية أويلر.
٦- الأس الثنائي (ربع و اضرب)
٧-اختبارات الأولية .

الباب ٥١

الخوارزمية الإقليدية:

تقوم هذه الخوارزمية بحساب القاسم المشترك الـأكبر للعددين (r_0, r_1) ، $gcd(r_0, r_1)$.

و تقوم بذلك باتباع الخطوات البسيطة التالية:

⋆ اختبار إذا كان $(r_1 == 0)$.

إذا كانت تلك هي الحالة عندئذ يكون r_0 الحالي هو الحل النهائي.

⋆ جعل $temp = r_1$.

⋆ جعل $r_1 = r_0 \bmod r_1$.

⋆ جعل $r_0 = temp$

⋆ إعادة ما سبق ضمنياً .

الباب ٦١

الخوارزمية الإقليدية الممددة:

على فرض :
$gcd(r_0, r_1) = 1$
النظرية تقول أنه يمكننا كتابة السطر السابق كما يلي :
. $gcd(r_0, r_1) = s * r_0 + t * r_1$
كما في الخوارزمية الإقليدية العادية نقوم بحساب gcd بشكل يستدعي نفسه و ذلك يجعل :
$r_i = r_{i-2} \pmod{r}_{i-1}$
$q_{i-1} = (r_{i-2} - r_i)/r_{i-1}$
$t_i = t_{i-2} - q_{i-1} * t_{i-1}$
حتى نصل إلى : $gcd(r_0, r_1) \equiv 1$
عند هذه النقطة :
$t = t_{i-1}$
الآن نخضع المعادلة إلى عملية باقي القسمة :
$gcd(r_0, r_1) \equiv 1 \equiv s * r_0 + t * r_1$
$1 \bmod r_0 \equiv (s * r_0 + t * r_1) \bmod r_0$
$1 \bmod r_0 = t * r_0 \bmod r_0$
و بما أن :
$1 \bmod r_0 \equiv r_1^{-1} * r_1 \bmod r_0$
يكون :
$r_1^{-1} \equiv t$
و هذه طريقة أولى لحساب معكوس باقي القسمة .

الباب ٧١

التابع فاي ϕ :

ليكن لدينا مجموعة من الأعداد الصحيحة $0, 1, 2, \ldots, m-1$. كم عدد الأعداد في المجموعة التي هي أولية فيما بينها ل m ؟
الجواب: تابع ϕ ل أويلر .
مثال للمجموعة m = 5: [**0,1,2,3,4**])

$$gcd(0,5) = 5$$
$$gcd(1,5) = 1$$
$$gcd(2,5) = 1$$
$$gcd(3,5) = 1$$
$$gcd(4,5) = 1$$

هذا يؤدي إلى أن :

$$\phi(5) = 4$$

(m=6) [**0,1,2,3,4,5**]

$$gcd(0,6) = 6$$
$$gcd(1,6) = 1$$
$$gcd(2,6) = 2$$
$$gcd(3,6) = 3$$
$$gcd(4,6) = 2$$
$$gcd(5,6) = 1$$

و من هنا

$$\phi(6) = 2$$

هذه الطريقة بحساب القاسم المشترك الأكبر لأعداد المجموعة من 0 إلى m-1 مع m بطيئة جدا من اجل الاعداد الكبيرة .
إذا كان لدينا تحليل إلى عوامل اولية للعدد m:

$$m = p_1^{e_1} * p_2^{e_2} * .... * p_n^{e_n}$$

نحسب التابع ϕ وفقا للعلاقة

$$\phi(m) = \prod_{i=1}^{n}(p_i^{e_i} - p_i^{e_{i-1}})$$

ϕ سهل من أجل $e_i = 1$ خصوصا
مثلا : $m = p \; . \; q$
p,q عددين أوليين .
و منه : $\phi(m) = (p-1) * (q-1)$

ملاحظة:ايجاد $\phi(m)$ هو سهل حسابيا اذا كانت العوامل الأولية ل m معلومة.
(من ناحية أخرى حساب $\phi(m)$ يصبح شبه مستحيل للأعداد الكبيرة).

الباب ٨١

نظرية فيرمات الصغيرة:

ليكن لدينا عدد أولي p و وعدد صحيح a
عندئذ تقول النظرية :
$a^p \equiv a \bmod p$
ويمكن إعادة كتابة المعادلة السابقة بالشكل : $(a^{p-1} \equiv 1 \bmod p)$
تقول هذه النظرية إن العدد p الذي يجتاز الاختبار السابق هو عدد أولي محتمل .

استخدامها :

تعطي معكوس باقي القسمة ، إذا كان p عدد أولي ، ونستطيع كتابة المعادلة بالشكل :
$a \ * \ a^{p-2} \equiv 1 \bmod p$
تقارن مع تعريف معكوس باقي القسمة
$a * a^{-1} \equiv 1 \bmod p$
$a^{-1} \equiv a^{p-2} \bmod p$

مثال :

$a = 2, \ p = 7$
$a^{p-2} = 2^5 = 32 \equiv 4 \bmod 7$
$Verify : 2 * 4 \equiv 1 \bmod 7$
نظرية فيرمات الصغيرة تعمل فقط بالشكل a أولي بالنسبة ل p

الباب ٩١

نظرية أويلر :

تستخدم لتعميم نظرية فيرمات الصغيرة على أي عددين صحيحين أوليين
فيما بينهما a و m
$a^{\phi(m)} \equiv 1 \bmod m$

مثال :

أحسب تابع فاي لأويلر من أجل m=12, a=5

$$\phi(12) = \phi(2^2 * 3) = (2^2 - 2^1)(3^1 - 3^0) = (4-2)(3-1) = 4$$

تحقق من نظرية أويلر

$$5^{\phi(12)} = 5^4 = 25^2 = 625 \equiv 1 \bmod 12$$

نظرية فيرمات الصغيرة هي حالة خاصة من نظرية أويلر

من أجل العدد الأولي p في نظرية أويلر :

$$\phi(p) = (p^1 - p^o) = p - 1$$

و في نظرية فيرمات :

$$a^{\phi(p)} = a^{p-1} \equiv 1 \bmod p$$

الباب ٠٢

ربع و اضرب :

المبدأ الأساسي :تفحص بتات الأس من اليسار إلى اليمين وربع أو اضرب وفقا لخوارزمية التربيع والضرب من أجل $x^h \bmod n$

الدخل : الأساس x و الأس h و باقي القسمة n .

الخرج : $y = x^h \bmod n$
١)⋆ تحديد التمثيل الثنائي ل h .
$h = (\ h_i, h_{i-1}, ...h_o)_2$
٢⋆ من أجل t =*i-1* و حتى ال 0 .
٣⋆ $y = y^2 \bmod n$
٤⋆ إذا كان $h_t = 1$ يكون :
٥⋆ $y = (y * x) \bmod n$
٦⋆ أعد قيمة y .
قاعدة :

⋆ ربع في كل تكرار (الخطوة 3) واضرب النتيجة الحالية ب x إذا كان بت الاس h_t يساوي الواحد (خطوة 5)
⋆ التخفيض بعد كل خطوة يحافظ على المعامل y صغيراْ .

الباب ١٢

اختبار الأولية :

هناك العديد من الطرق لتحديد فيما إذا كان p هو عدد أولي ام لا .
إحدى الطرق لتحديد ذلك هي تحليل p إلى عوامله الأولية .
والطريقة الأخرى هي بالاعتماد على قواعد المساواة التي تنطبق فقط على الأعداد الأولية واختبار إذا كانت تنطبق هذه القواعد على p أم لا فإذا تحقق ذلك يكون p على الأرجح أولي وإذا لم يتحقق فمن المؤكد أنه مركب .

الباب ٢٢

استخدام المناخل من أجل التحليل إلى عوامل أولية :

المناخل هي طريقة ممتازة لتوفير الوقت اللازم لاختبار الأولية من أجل حالات اختبار متعددة .
المنخل هو مصفوفة منطقية تستخدم الفهارس للإشارة إلى العدد الذي نريد تخزينه وتستخدم قيمة منطقية للإشارة إلى الأولية
(في حالة 1 العدد أولي ، و في حالة 0 العدد مركب) .
يتم تهيئة المصفوفة طبقا للحالة 1 ، أي أن الحالة البدائية تعتبر أن جميع الداد أولية .
نبدأ بالرور عبر الأرقام (الفهارس) . من أجل كل فهرس يحتوي على القيمة 1 افعل التالي : ⋆ المرور عبر جميع الفهارس التي هي من مضاعفات الفهرس الاولي وتبديل قيمتها بالقيمة 0 .

خدع المنخل :

١ بالنسبة إلى فهرس أولي معطى ، كل مضاعقات هذا الفهرس حتى Index^2 يتم تبديلها إلى أعداد مركبة (جعل قيمتها 0) من خلال مرورات الفهارس الأولية السابقة .
لذلك : فقط بدل مضاعفات الفهارس الأولية التي هي أكبر من Index^2
٢⋆ كل الفهارس الأولية التي نحتاجها لتحديد أولية فهرس معين هي تحت جذر ذلك الفهرس $\sqrt{Index}$
لذلك استمر بالمرور على الفهارس الأولية حتى تصل إلى جذر الحد الأعلى في المصفوفة $\sqrt{array_{limit}}$

بشكل عام :

المنخل هو طريقة لتصفية الاعداد الأولية من عينة من الاعداد ضمن مجال معين.
المنخل التقليدي يقوم بتصفية الاعداد الأولية ضمن مجال يبدأ من الصفر و حتى عدد معطى.

المنخل المقسم يستخدم خواص رياضية تتعلق بأعداد أولية بحيث يقوم بتصفية الأعداد الأولية من عدد معطى و حتى عدد معطى آخر .

الباب ٣٢

قواعد الأعداد الأولية :

على فرض أن العدد p أولي ، عندئذ يمكن أن نكتب :

$P = (r_1 * r_2 * .... * r_i) + 1$

حيث أن r1.....ri عوامل أولية ل p-1

نأخذ عدد عشوائي a حيث :

a < P و a > 1

فيكون : gcd(P, a) = 1

الآن أوجد نتيجة المعادلة التالية :

$\mathrm{a}^{p-1} =? \bmod P$

$\mathrm{a}^{(r_1 * r_2 * .... * r_i)} =? \bmod P$

$((\mathrm{a}^{r_1})^{r_2})^{r_i} =? \bmod P$

من أجل :

$\text{answer} = (\mathrm{a}^{r_i} \bmod P) \in [1...P-1]$

لدينا $p-1$ محاولة ، و كل محاولة تنتج answer مختلف(حيث أن عملية باقي القسمة دورية و

$gcd(P, a) = 1$

حتى نصل إلى $\mathrm{a}^{r_i} = 1 \bmod P$

عند تلك النقطة

$1^{r_i} \equiv 1 \bmod P$

ما سبق يثبت صحة نظرية فيرمات الصغيرة. اذا اجتاز عدد معطى معين هو p القوانين السابقه فانه عدد أولي محتمل.

ولكن ايضا اذا اعتبرنا a^p

،بعد بضع خطوات من المعالجة الرياضية نستنتج أن: $\mathrm{a}^p \equiv a \bmod p$

اذا ضربنا الطرفين ب a^{-2} :

$\mathrm{a}^p * a^{-2} \equiv a * a^{-2} \bmod p$

$\mathrm{a}^{p-2} \equiv a^{-1} \bmod P$

و هذه طريقة ثانية لحساب معكوس باقي القسمة.

الباب ٤٢

خوارزمية ال RSA :

نشرت الورقة الأولية التي تشرح المفتاح العمومي من قبل مارتن هيلمان و ويتفلد ديفي في عام 1976 .
ثم وضعت أسس هذه الخوارزمية في عام 1977 من قبل رونالد ريفيست ، ايدي شامير و لينارد ادلمان .
انها خوارزمية التشفير غير المتناظر الاكثر استخداما.
على الرغم من أن التشفير باستخدام منحني القطع الناقص ECC بدأ يأخذ شعبية .

استخداماتها:

١- نقل مفاتيح خوارزميات التشفير المتناظرة على شبكة غير آمنة.
٢- التواقيع الرقمية.

الباب ٥٢

التشفير و فك التشفير :

تتم عمليات ال RSA في حلقة الأعداد الصحيحة Z_n .
$Z_n(\mathrm{mod}\, n)$
حيث $n = p * q$ حيث p , q أعداد أولية .
ينفذ التشفير وفك التشفير في الحلقة ببساطة .

تعريف :

يتم التشفير من خلال رفع الرسالة الى أس المفتاح العمومي وأخد باقي قسمته.
⋆بينما يتم فك التشفير من خلال رفع الرسالة المشفرة الى أس المفتاح الخصوصي و أخذ باقي قسمته.
حيث أن المقسوم عليه هو ناتج ضرب عددان أوليان كبيران .
من أجل المفتاح العمومي يجب تحديد n , e .
و من أجل المفتاح الخصوصي نكتب :

$$y = e_{kpub}(x) \equiv x^e \bmod n$$

$$x = d_{kpr}(y) \equiv y^d \bmod n$$

عندما x , m , y أعداد صحيحة .
نستدعي التابع e_{kpub} في عملية التشفير ونستدعي التابع d_{kpr} في عملية فك التشفير .
في التطبيق يكون x , y , n ,d أعداد صحيحة كبيرة جدا (أكبر من 1024 بت)
أمن النظام يعتمد على أنه من الصعب استخلاص عناصر المفتاح الخصوصي d من المفتاح العمومي يعطي فقط n , e .

الباب ٦٢

توليد المفاتيح :

كما في جميع المخططات غير المتناظرة تقوم خوارزمية ال RSA بمجموعة من الخطوات خلال حساب المفتاح العمومي والمفتاح الخصوصي كالتالي :

⋆١ نختار عددان أوليان كبيران :

$$p \ , \ q$$

⋆٢ نحسب ناتج ضربهما

$$n = p \ * \ q$$

⋆٣ نحسب نتيجة تابع ϕ لهما

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

⋆٤ نختار مفتاح عمومي $\mathrm{e} \in 1, 2, ..., \phi(n) - 1$ أصغر من ϕ و القاسم المشترك الأكبر له مع ϕ هو الواحد

$$gcd(e, \ \phi(n)) = 1$$

⋆٥ نحسب المفتاح الخصوصي عن طريق الخوارزمية الاقليدية الممددة

$$d \ * \ e \equiv 1 \bmod \phi(n)$$

⋆٦ إعادة

$$k_{pub} = (n, e), k_{pr} = d$$

ملاحظات :

⋆ اختيار عددين أوليين كبيرين p , q ليس بالأمر السهل .

⋆ $(\ gcd(e, \ \phi(n)) = 1)$

يضمن أن e له معكوس و بالتالي يوجد دائما مفتاح خصوصي d .

الباب ٧٢

نقاط قوة ال RSA :

⋆ لحساب المفتاح الخصوصي يجب أن يكون لدينا نتيجة التابع ϕ .
⋆ لحساب نتيجة ϕ يجب أن يكون لدينا كل من العددان الأوليان الكبيران p , q .

⋆ الطريقة الوحيدة للحصول على العددين الأوليين من قناة غير آمنة هي بالحصول على نتيجة ضربهما n (و هذه النتيجة بالأساس عمومية).
⋆ للحصول على العددين الأوليين من ناتج ضربهما يجب تحليله الى عوامله الأولية و ذلك غير ممكن من أجل أعداد صحيحه ذات 1024 خانه باستخدام القدرات الحوسبية الحالية .

الباب ٨٢

إشكاليات ال RSA :

١- اختيار مفتاح عمومي صغير e يعرض الرسالة المشفرة بعد رفعها للأس للبقاء كما هي عند إخضاعها لعملية باقي القسمة مما يمكن المخترقين من فك تشفيرها بأخذ الجذر للمفتاح العمومي للرسالة المشفرة.

أي على فرض : e مفتاح عمومي

إذا كان : $modulus$ ¡ $\mathrm{message}^e$

فإن :

$$message^e \equiv message^e \bmod modulus$$

و الرسالة يمكن إعادة توليدها من قبل المخترقين باستخدام المعادلة :

$$\mathrm{message} = \sqrt[e]{message^e}$$

الحل:

تفادي الأعداد الصغيرة نسبيا عند اختيار مفتاح عمومي.

٢- المخترقين يستطيعون مقارنة نص متوقع يقومون بتشفيره باستخدام المفتاح العمومي مع النص الأساسي المشفر .

الحل:

نبطين الرسالة النصية قبل تشفيرها بقيم عشوائية .

الباب ٩٢

يتضمن تطبيق ال EnDaBi :

⋆ مكتبة نواة ال RSA لل $EnDaBi$.
⋆ برنامج عرض بدون واجهة يستعرض التوابع الرئيسية للمكتبة.
⋆ برنامج عرض مع واجهة يستعرض التوابع الرئيسية للمكتبة .
⋆برنامج مثال عن المنخل المقسم.
⋆ برنامج جافا صغير يستخدم اختبار أولية مبني داخليا.
⋆ ملف صنع ، يستخدم لبناء البرامج.

الباب ٠٣

النظرة المستقبلية للمشروع :

**** فيما يخص نواة ال** RSA :

١- تطبيق نظرية الباقي الصيني من أجل أسية المفتاح الخصوصي بشكل أسرع (فك التشفير).

٢- تطبيق مكتبة أعداد كبيرة خاصة بنا .

٣- تطبيق نظام تبطين خاص بنا .

٤- تطبيق أصناف اختبارات أولية خاصة بنا .

****فيما يخص المشروع** :

١- إضافة تقنيات تشفير أخرى .

٢- تطوير أصناف قواعد بيانات .

٣- تطوير أصناف قياسات بيومترية .

الباب ١٣

لغات البرمجة المستخدمة :

C++ :

لغة برمجة متطلبات كتابتها قاسية ، و الأنواع فيها محددة سريعة و فعالة
يمكن تمديدها عبر المكتبات .

D :

لغة برمجة متطلبات كتابتها قاسية ، و الأنواع فيها محددة ، سريعة و فعالة ،
مع طريقة كتابة مشابهة للجافا و ال $C++$.

JAVA :

لغة برمجة متطلبات كتابتها قاسية ، و الأنواع فيها محددة ، سريعة و فعالة ،
يمكن ترجمتها إل البايت كود تتمتع بقابلية الحمل بشكل ملفات قابلة
للتنفيذ (ترجم مرة واحدة شغل في كل مكان) .

FLTK :

عدة العمل السريعة و الخفيفة تلفظ فولتيك و هي عدة عمل لواجهات
المستخدم الرسومية مخصصة للغة ال $C++$
و تعمل على أنظمة التشغيل :
X Window System, MacOS, and Microsoft Windows
بعد تنزيل دعم ال .OpenGL

EnDaBi RSA DEMO GUI مبني جزئيا على أعمال مشروع الفولتيك ،
http://www.fltk.org.

LaTeX :

نظام كتابة عالي الجودة يتضمن صفات صممت من أجل إنتاج التوثيق العلمي
و التقني
و *LaTeX* هو المعيار بالخبرة من أجل نشر و طباعة التوثيق العلمي .

<u>InfInt :</u>

مكتبة حساب الأعداد الصحيحة غير ذات دقة الفاصلة .
مرخصة تحت رخصة : *LGPL 2.1* .

code.google.com/p/infint/

الباب ٢٣

البرامج المستخدمة :

Ubuntu 14.04 LTS :

نظام تشغيل مبني على $Linux$ حر و مفتوح المصدر .

GCC :

مترجم C , C++ من مشروع GNU .

GDC :

مترجم لغة D من GNU .

Javac :

مترجم للغة البرمجة $JAVA$.

TeXstudio :

محرر $LaTeX$ مع واجهة مستخدم رسومية .

Code::Blocks :

IDE مفتوح المصدر و يعمل على عدة منصات .

SciTE :

محرر نصي للمبرمجين .

Vim :

محرر نصي متوافق مع VI يمكن استخدامه لتحرير جميع أنواع النصوص المجردة و هو بشكل خصوصي مناسب لتحرير البرامج .

Eclipse :

IDE قابل للتمديد و هو يستخدم لتطوير برمجيات $JAVA$ و أدوات لنظم التشغيل .

: <u>nano</u>

محرر نصي خفيف و مجاني يستبدل محرر ال $PICO$ و هو المحرر الإفتراضي في حزمة برمجيات $PINE$.

: <u>make</u>

أداة بناء من مشروع GNU تستخدم لتطوير مجموعة من البرمجيات .

: <u>Git</u>

نظام تحكم بالنسخ ، موزع سريع يمكن تطويره غني بالتعليمات يوفر الوصول إلى تعليمات عالية المستوى ووصول تام إلى داخليات البرامج .

: <u>yEd</u>

برنامج سطح مكتب قوي يمكن استخدامه للتطوير السريع و الفعال لبناء مخططات عالية النوعية .

الباب ٣٣

كيف تستخدم برمجياتنا؟

*١ عملية التنزيل تم اختارها على *Ubuntu 14.04 LTS.* .
*٢ حمل متطلبات التنزيل .
*٣ اسحب الرماز المصدري لمشروع *EnDaBi* من *GETHUB* .
*٤ اذهب إلى مجلد *EnDaBi* .
*٥ ترجم الرماز المصدري .
*٦ شغل برامج العروض .

الباب ٤٣

ملحق :

المصادر

كتاب فهم التشفير (كتاب للمهندسين و الطلاب) ل **كريستوف بار** و **جان بيلتذل** .