Understanding Cryptography

Answers of Homework No.4

Chapter 7

Chinese remainder theorem

1. Let m_1 and m_2 be two positive integers that are relatively prime. Given any two integers a and b, there exists an integers x such that

$$\boldsymbol{x \equiv a \quad (mod \quad m_1)}$$
$$\boldsymbol{x \equiv b \quad (mod \quad m_2)}$$

Prove any two solutions of these equations are congruent to each other modulo $m_1 m_2$.

حل:

طبق صورت مساله می دانیم که $\gcd(m_1, m_2) = 1$ است. در اینجا فرض کرده که به جز x ، مقدار y نیز جوابی برای دستگاه زیر باشد:

$$\begin{cases} x \equiv a \quad mod\ m_1 \\ x \equiv b \quad mod\ m_2 \end{cases} \qquad \begin{cases} y \equiv a \quad mod\ m_1 \\ y \equiv b \quad mod\ m_1 \end{cases}$$

$$\begin{cases} x = y \quad mod\ m_1 \\ x = y \quad mod\ m_2 \end{cases} \quad \rightarrow \quad \begin{cases} x - y = m_1 \times k \\ x - y = m_2 \times k' \end{cases} \rightarrow \quad k(m_1 m_2) = x - y$$

$$x = k(m_1 m_2) + y \qquad \rightarrow \qquad x \equiv y\ (mod\ m_1 m_2)$$

Fermats little theorem

2. Let p be a prime. then prove for every positive integer a:

$$\boldsymbol{a^p \equiv a \ (mod\ p)}$$

$$\boldsymbol{(x + y)^p \equiv x^p + y^p \quad (mod\ p)}$$

حل:

ابتدا لم دوم را اثبات خواهیم کرد سپس از آن برای اثبات لم اول استفاده خواهیم نمود.

اثبات لم دوم:

با فرض اینکه p یک عدد اول و ضرایب چند جمله ای برای $0 < i < p$ داریم:

$$\binom{p}{i} = \frac{p!}{(p-i)!\,i!}$$

که $p > i \;,\; p > p - i$ است. به دلیل اینکه p عدد اول می باشد، $\binom{p}{i}$ توسط p قابل تقسیم است. در نتیجه $\binom{p}{i}$ با شرط $0 < i < p$ در پیمانه p به صفر همگرا می شود.

طبق قضیه دو جمله ای داریم:

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i}\, y^i$$
$$= \binom{p}{0} x^p + \binom{p}{1} x^{p-1} y + \binom{p}{2} x^{p-2}\, y + \ldots + \binom{p}{p-1} x\, y^{p-1} + \binom{p}{p} y^p$$

همه عبارت های میانی بالا (به جز ترم اول و آخر) به پیمانه p به صفر همگرا می شوند.

$$\binom{p}{0} = \binom{p}{p} = 1$$

در نتیجه داریم:

$$\boldsymbol{(x+y)^p \equiv x^p + y^p \pmod{p}}$$

اثبات لم اول:

گام اول : اگر $a = 1$ باشد داریم:

$$a^p = 1^p = 1 = a$$

پس به ازای $a = 1$ نتیجه برقرار است.

در گام دوم (فرض استقرا) فرض می‌کنیم که $k^p \equiv k \pmod{p}$ برقرار است و نتیجه می‌گیریم که $(k+1)^p = (k+1)$ به عنوان حکم استقرا اثبات میشود.

می توان از لم اول که در قسمت بالا اثبات گردید استفاده کنیم.

$$(k+1)^p \equiv k^p + 1 \qquad (mod\; p)$$

و داریم:

$$(k+1)^p \equiv k + 1 \pmod{p}$$

پس برای هر عدد صحیح مثبتی مثل a داریم :

$$a^p \equiv a \pmod p$$

Chapter 8

Diffie- Hellman Key Exchange

3. In the DHKE protocol, the private keys are chosen from the set $\{2, \ldots, p-1\}$. Why are the values 1 and $p-1$ are not considered?

NOTE: Describe the weakness of those two values.

حل:

عدد 1 یک کلید ضعیف است. وقتیکه به عنوان کلید خصوصی استفاده شود، کلید عمومی ایجاد شده مساوی با α می گردد. در این صورت به مهاجم این اجازه را می دهد که کلید خصوصی را به دست آورد.
همچنین $p-1$ نیز یک کلید ضعیف است. چون $\alpha^{p-1} \bmod p \equiv 1$ به ازای هر α برقرار است. با توجه بعد عدد اول بودن p این به مهاجم اجازه می‌دهد که کلید خصوصی را به دست آورد.

4.1. Compute the two public keys and the common key for the DHKE scheme with the parameters $p = 467$, $\alpha = 2$, $a = 228$, $b = 57$.

4.2. We now design another DHKE scheme with the same prime $p = 467$ as in problem 4.1. this time, we use the element $\alpha = 4$. The element 4 has order 233 and generates a subgroup with 233 elements. Compute k_{AB} for :

$$\boldsymbol{a = 400 , b = 134}$$

حل:

4.1.

$$a = 228, b = 57$$

$Alice$:

$$k_{pr,A} = 228$$

$$\begin{aligned} k_{pub,A} = \alpha^a \bmod p &= 2^{228} \bmod 467 = 2^{9\times25+3} \bmod 496 \\ &= 45 \times 45 \times \ldots .45 \times 8 \bmod 467 \\ &= (45)^{2\times12} \times 45 \times 8 \bmod 467 = 157^{12} \times 45 \times 8 \bmod 467 \\ &= 365^6 \times 45 \times 8 \bmod 467 = 130^3 \times 45 \times 8 \bmod 467 \\ &= 88 \times 246 \times 8 \bmod 467 = 394 \bmod 467 = A \end{aligned}$$

Bob:

$$k_{pr,B} = 57$$

$$k_{pub,B} = \alpha^b \ mod\ p = 2^{57} \ mod\ 467 = 2^{9\times6+3}\ mod\ 467$$
$$= 45^6 \times 8 \ mod\ 467 = 157^3 \times 8 \ mod\ 467$$
$$= 365 \times 157 \times 8 \ mod\ 467 = 313 \ mod\ 467 = B$$

با مبادله شدن کلید A و B داریم:

$$k_{AB} = \left(k_{pub,A}\right)^b \ mod\ p = 394^{57} \ mod\ 467 = 394^{3\times19} \ mod\ 467$$
$$= 461^{19} \ mod\ 467 = 461^{2\times9} \times 461 \ mod\ 467$$
$$= 36^9 \times 461\ mod\ 467 = 423^3 \times 461 \ mod\ 467$$
$$= 68 \times 264 \ mod\ 467 = 206\ mod\ 467$$

$$k_{BA} = \left(k_{pub,B}\right)^a \ mod\ p = 313^{228} \ mod\ 467 = 206$$

$$k_{AB} = k_{BA}$$

4.2.

$$p = 467 \quad ,\alpha = 4$$
$$a = 400 \quad ,b = 134$$

$Alice$:

$$k_{pr,A} = 400$$

$$k_{pub,A} = \alpha^a \ mod\ p \equiv 4^{400} \ mod\ 467 = 89 = A$$

Bob:

$$k_{pr,B} = 134$$

$$k_{pub,B} = \alpha^b \ mod\ p \equiv 4^{134} \ mod\ 467 = 51 = B$$

قسمت 4.3 نیازی به حل نیست و جزء بارم بندی محسوب نمی‌شود.

Primitive Roots

5. Find a primitive root module 11, modulo 11^2 , modulo 2.11^2, and modulo 11^{100} .

حل:

منظور از $primitive\ root$ یک عدد مثل p عددی مثل a است که باقیمانده توان‌های a یعنی $(a^0,..,a^{p-1})$ به پیمانه p همه اعداد 1 تا $p-1$ را شامل گردد.

ابتدا باید بررسی کنیم آیا عدد ۲ یک $primitive\ root$ به پیمانه 11 هست یا نه؟ اردر ۲ برابر ۱۰ است چون توان های ۲ همه ی اعداد ۱ تا ۱۰ را می سازد. دیده می‌شود که $2^5 \not\equiv 1(mod\ 11)$

$2^2 \not\equiv 1 \pmod{11}$ بنابراین به ۲ و ۵ قابل تقسیم است. بنابراین، اردر دو باید ۱۰ باشد پس ۲ یک *primitive root* به پیمانه ۱۱ است.

به بیانی دیگر:

$\varphi(11) = 10$ می‌باشد. تعداد *primitive* های پیمانه عدد ۱۱، برابر $\varphi(10)$ است:

$\varphi(10) = 10\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 4$ است. پس 4 المان *primitive* دارد. طبق این قضیه که اگر α یک مولد از z_{11}^* باشد در نتیجه $b = \alpha^i \bmod n$ نیز مولد دیگری از z_{11}^* است اگر و تنها اگر $\gcd(i, \emptyset(m)) = 1$ باشد.

$$\emptyset(10) = 4$$

اعداد 1,3,7,9 نسبت به ۱۰ اول اند.

جهت یافتن α ، طبق اینکه α عضو مولد Z_p^* است. اگر و تنهااگر $\alpha^{\varphi(p)/n} \not\equiv 1 \bmod 11$ که n از تجزیه $\varphi(p)$ به اعداد اول به دست می آید. پس داریم:

$$\alpha^5 \not\equiv 1 \quad mod\ 11$$
$$\alpha^2 \not\equiv 1 \quad mod\ 11$$

اگر $\alpha = 2$ باشد داریم:

$$2^5 \equiv 32 \quad mod\ 11 \equiv 10 \quad mod\ 11 \quad \surd$$
$$2^2 \equiv 4 \quad mod\ 11 \equiv \quad \surd$$

درنتیجه عدد ۲ یک مولد برای پیمانه ۱۱ است.

برای قسمت دوم مساله، می توانیم به راحتی محاسبه کنیم که

$2^{10} = 1024 \equiv 56 \pmod{11^2} \not\equiv 1\ mod\ 11^2$ پس این نشان می دهد که ۲ یک *primitive root* به پیمانه 11^2 هست.

پس نتیجه می‌شود که ۲ به طورکلی یک *primitive root* به پیمانه 11^d هست که مقدار $d \geq 2$ می‌باشد مثلا $d = 100$.

به بیانی دیگر: a یک عنصر *primitive* در پیمانه p است، اگر $a^{p-1} \not\equiv 1\ mod\ p^2$ باشد آن گاه a یک *primitive* در پیمانه p^2 است .

داریم: $\varphi(11^2) = 110 = 2 \times 5 \times 11$

اگر $\alpha = 2$ باشد داریم:

$$\alpha^2 \quad mod\ \ 11^2 \ \equiv\ 2^2 \quad mod\ \ 11^2 \equiv 4\ \ mod\ \ 11^2$$

$$\alpha^2 \quad mod\ \ 11^2 \ \equiv\ 2^5 \quad mod\ \ 11^2 \equiv 32\ \ mod\ \ 11^2$$

$$\alpha^{11} \quad mod\ \ 11^2 \ \equiv\ 2^{11} \quad mod\ \ 11^2 \equiv 2048\ \ mod\ \ 11^2 \equiv 112\ \ mod\ \ 11^2$$

پس نتیجه می شود که$\alpha = 2$ یک مولد در پیمانه 11^2 است.

بنابراین $\alpha = 2$ یک مولد در پیمانه 11 و 11^2 می باشد. داریم:

$$\varphi(2\times 11^2) = 2\times 11^2 \times \left(1-\frac{1}{11}\right)\times\left(1-\frac{1}{2}\right) = 11\times 10 = 110$$
$$= 2\times 5\times 11$$

اگر $\alpha = 2$

$$\alpha^2 \quad mod\ \ 2\times 11^2 \ \equiv\ 2^2 \quad mod\ 2\times 11^2 \ \equiv 4\ \ mod\ \ 2\times 11^2$$

$$\alpha^2 \quad mod\ \ 2\times 11^2 \ \equiv\ 2^5 \quad mod\ \ 2\times\ 11^2 \ \equiv 32\ \ mod\ \ 2\times\ 11^2$$

$$\alpha^{11} \quad mod\ \ 2\times 11^2 \ \equiv\ 2^{11} \quad mod\ \ 2\times 11^2 \ \equiv 2048\ \ mod\ \ 2\times 11^2$$
$$\equiv 112\ \ mod\ \ 2\times 11^2$$

نتیجه می شود که هر سه آیتم بالا مخالف یک می باشند پس $\alpha = 2$ یک $primitive$ یا مولد در پیمانه 2×11^2 است.

ElGamal Encryption System

6. If Bob uses ELGamal with $= 44927, a = 7, d = 22105$, find Bob's public key, encode the message $m = 10101$, and then decode the associated ciphertext.

حل:

ابتدا، کلید عمومی باب را محاسبه می کنیم:

$b = a^d \equiv 40909(mod\ p)$ پس کلید عمومی باب برابر $(p, a, b) = (44927{,}7{,}40909)$ است.

برای رمزنگاری، یک k تصادفی با $0 < k < p-1$ انتخاب می‌کنیم: به طور مثال $k = 6708$ ، سپس $r = a^k \equiv 12510\ (mod\ p)$ و $t = b^k m \equiv 12749\ (mod\ p)$ را محاسبه می کنیم. در نتیجه آلیس متن رمزشده زیر را به باب می فرستد.

$$(r, t) = (12510.12749)$$

برای رمزگشایی، باب مقدار $r^{-d} \equiv 11355(mod\ p)$ را محاسبه می کند و در t ضرب می کند تا مقدار $m = 10101$ را بدست آورد.

7.

- **CrypTool:**

1.

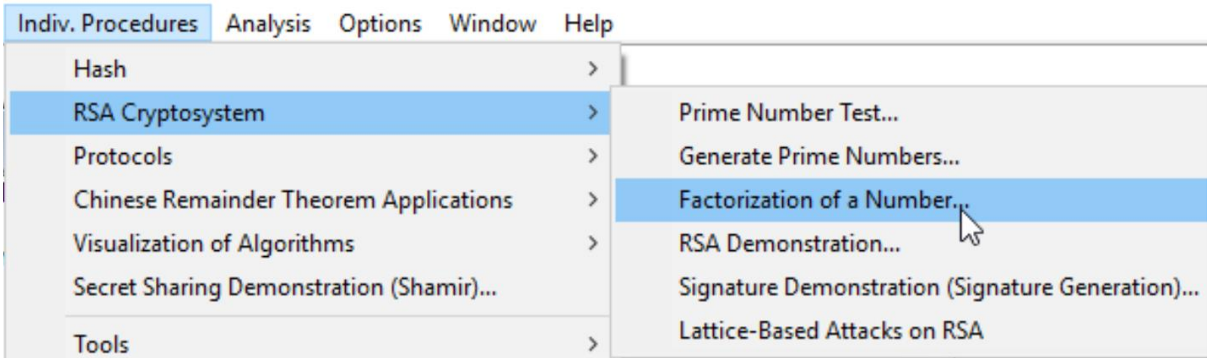

Figure 1: number factorization tool

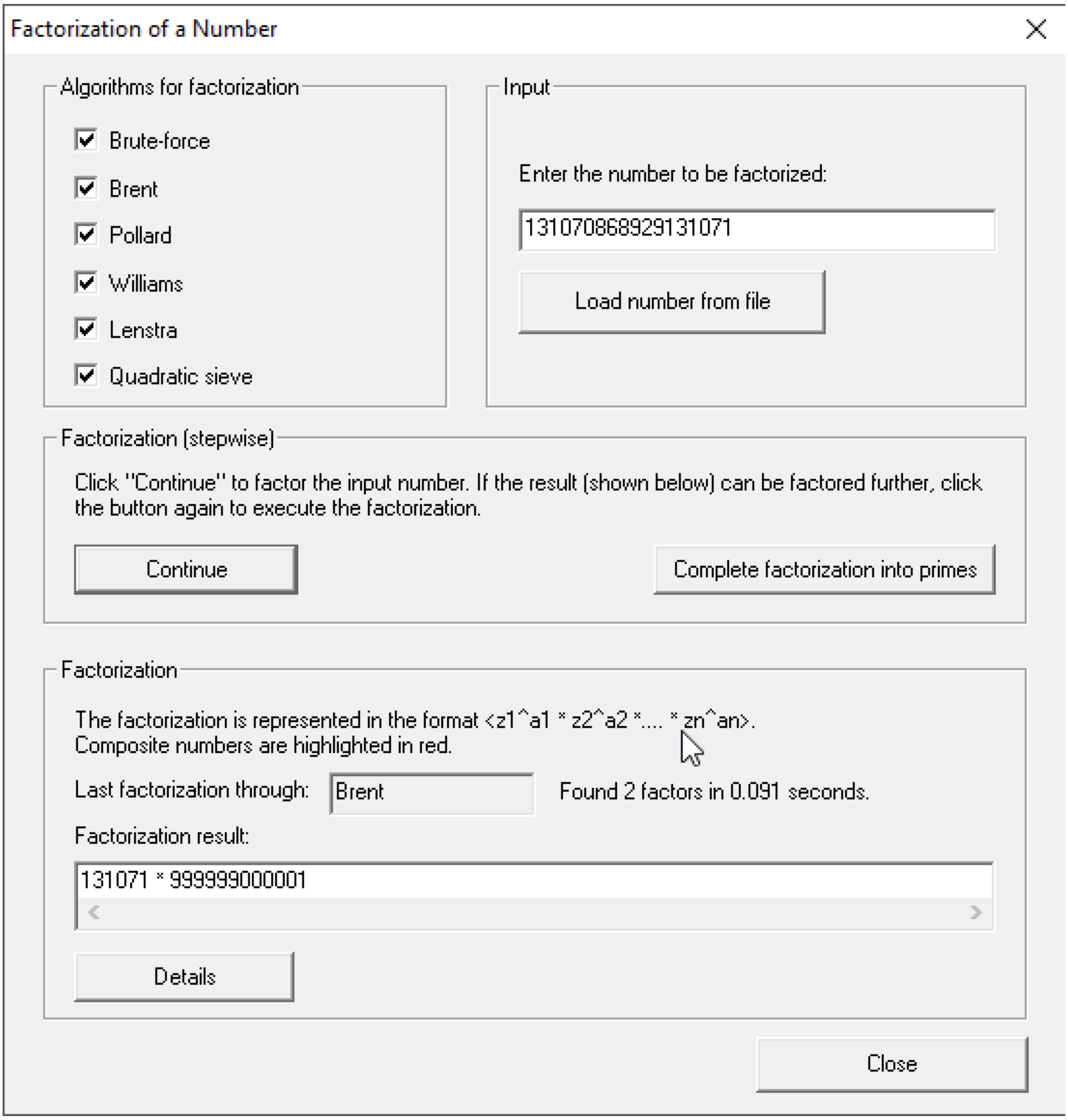

Figure 2: factoring the given number

2.

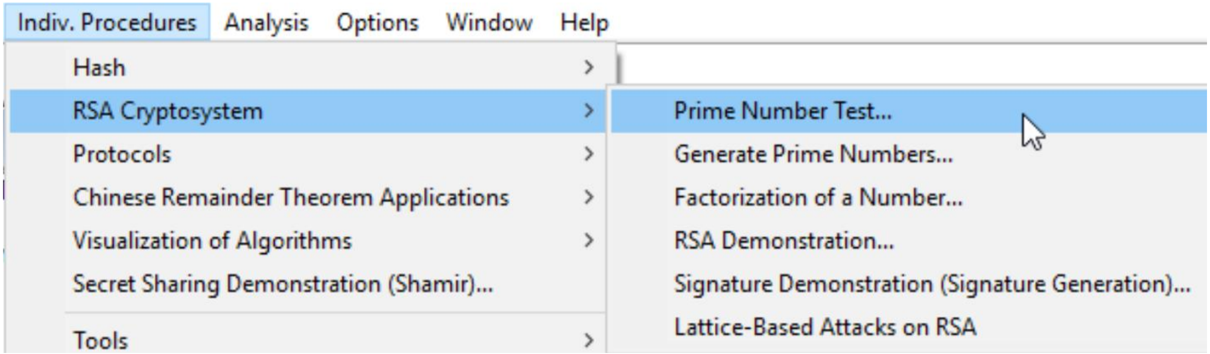

Figure 3: primality test tool

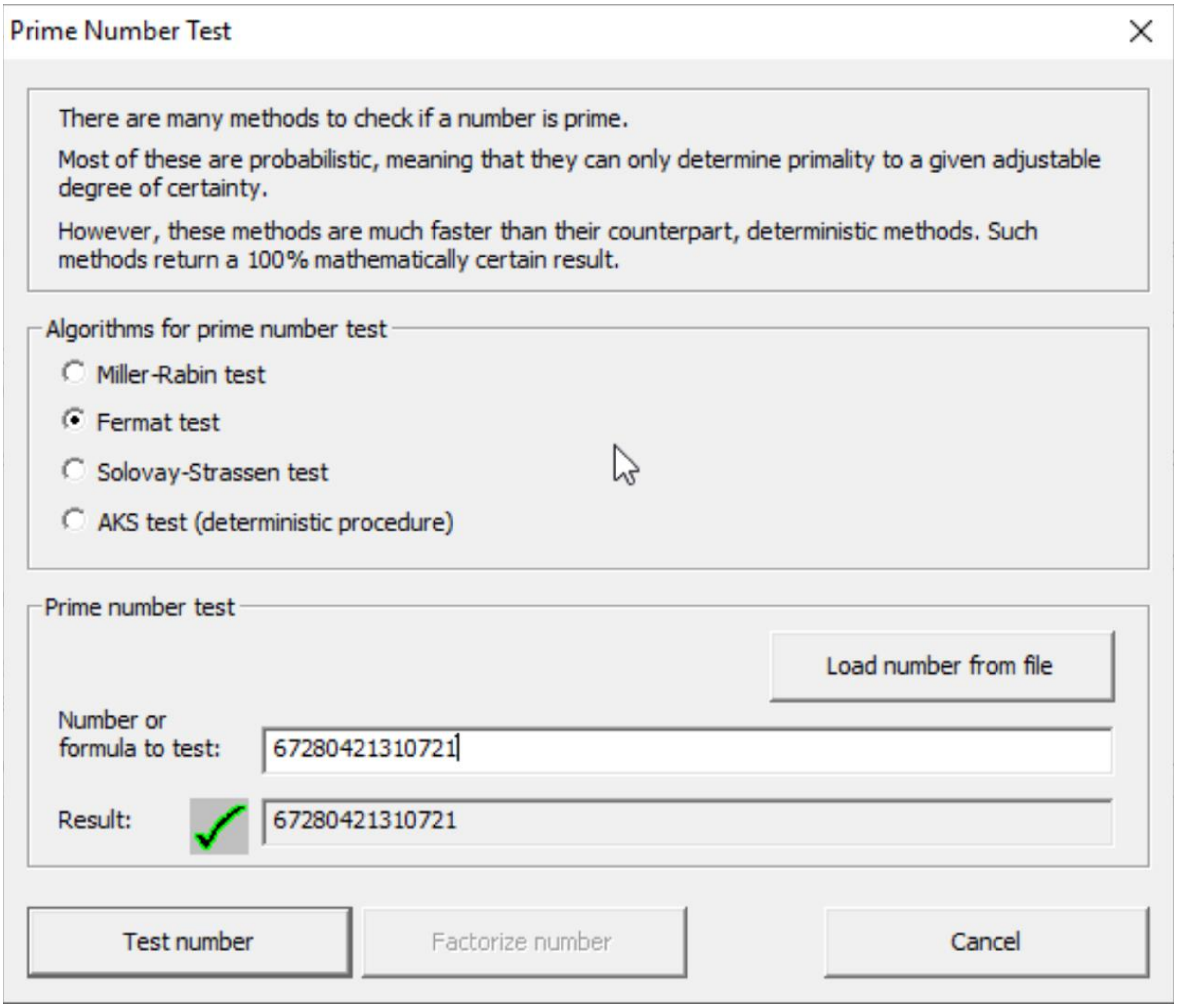

Figure 4: testing a prime number using Fermat test

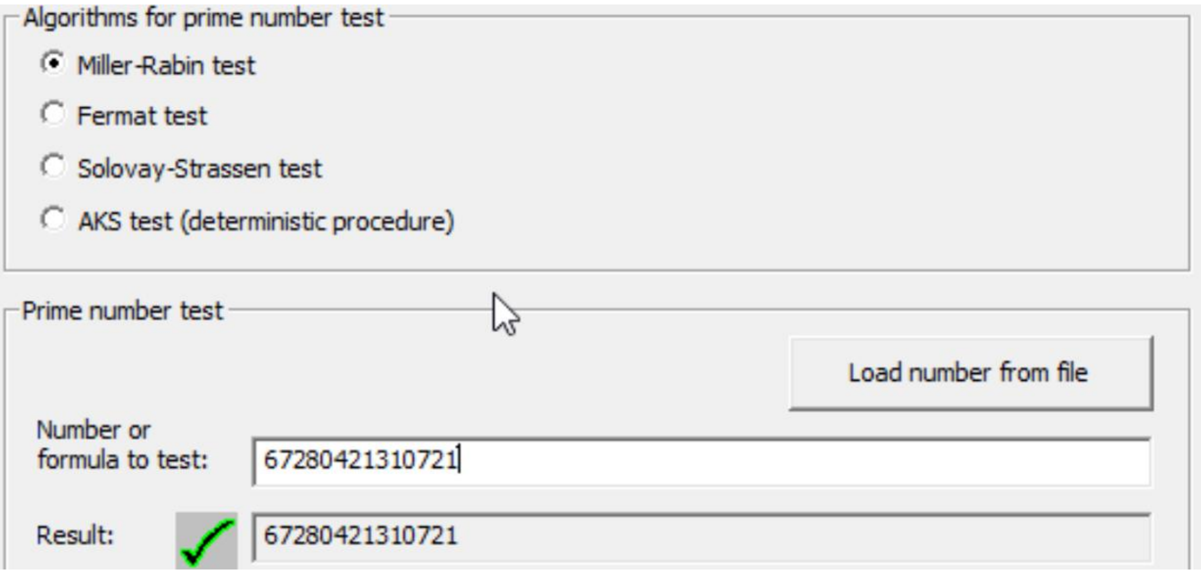

Figure 5: testing a prime number using Miller-Rabin test

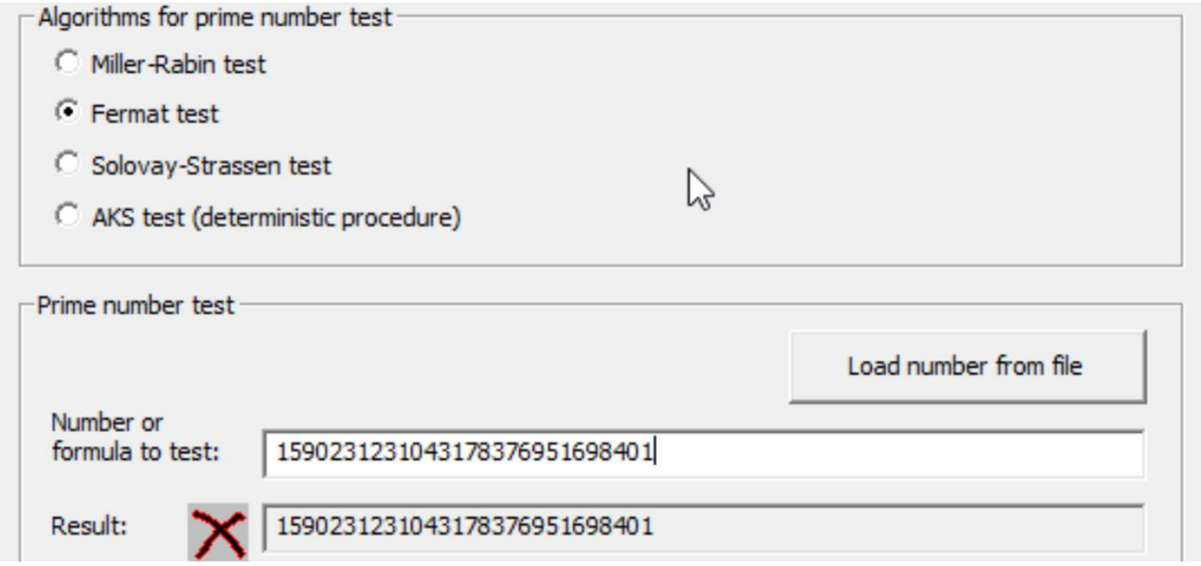

Figure 6: testing a Carmichael number using Fermat test

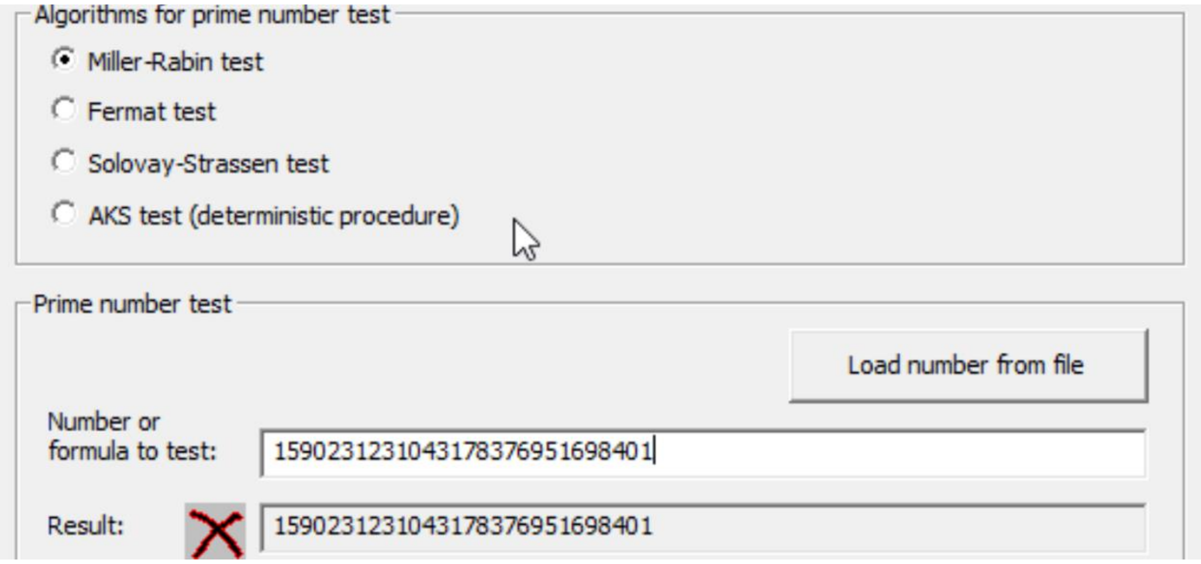

Figure 7: testing a Carmichael number using Miller-Rabin test

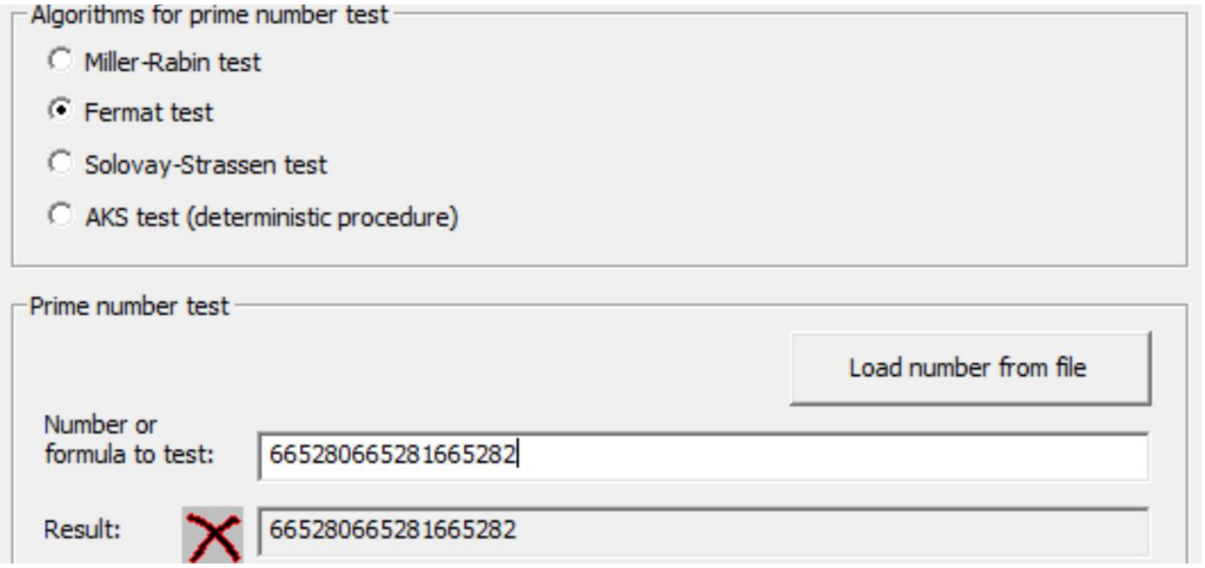

Figure 8: testing a composite number using Fermat test

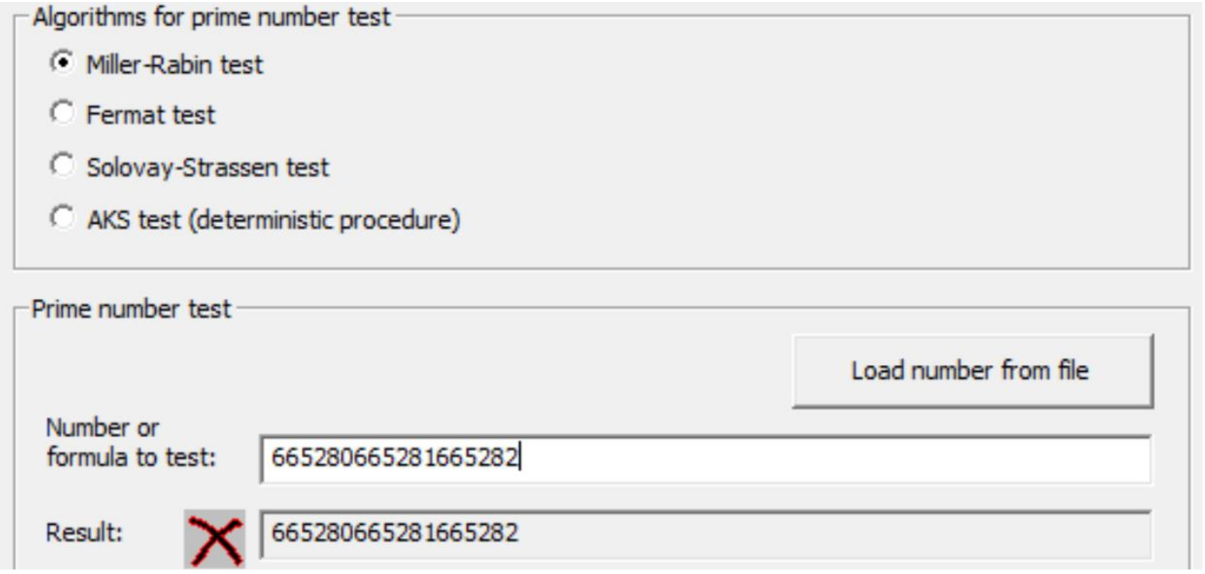

Figure 9: testing a composite number using Miller-Rabin test

3.

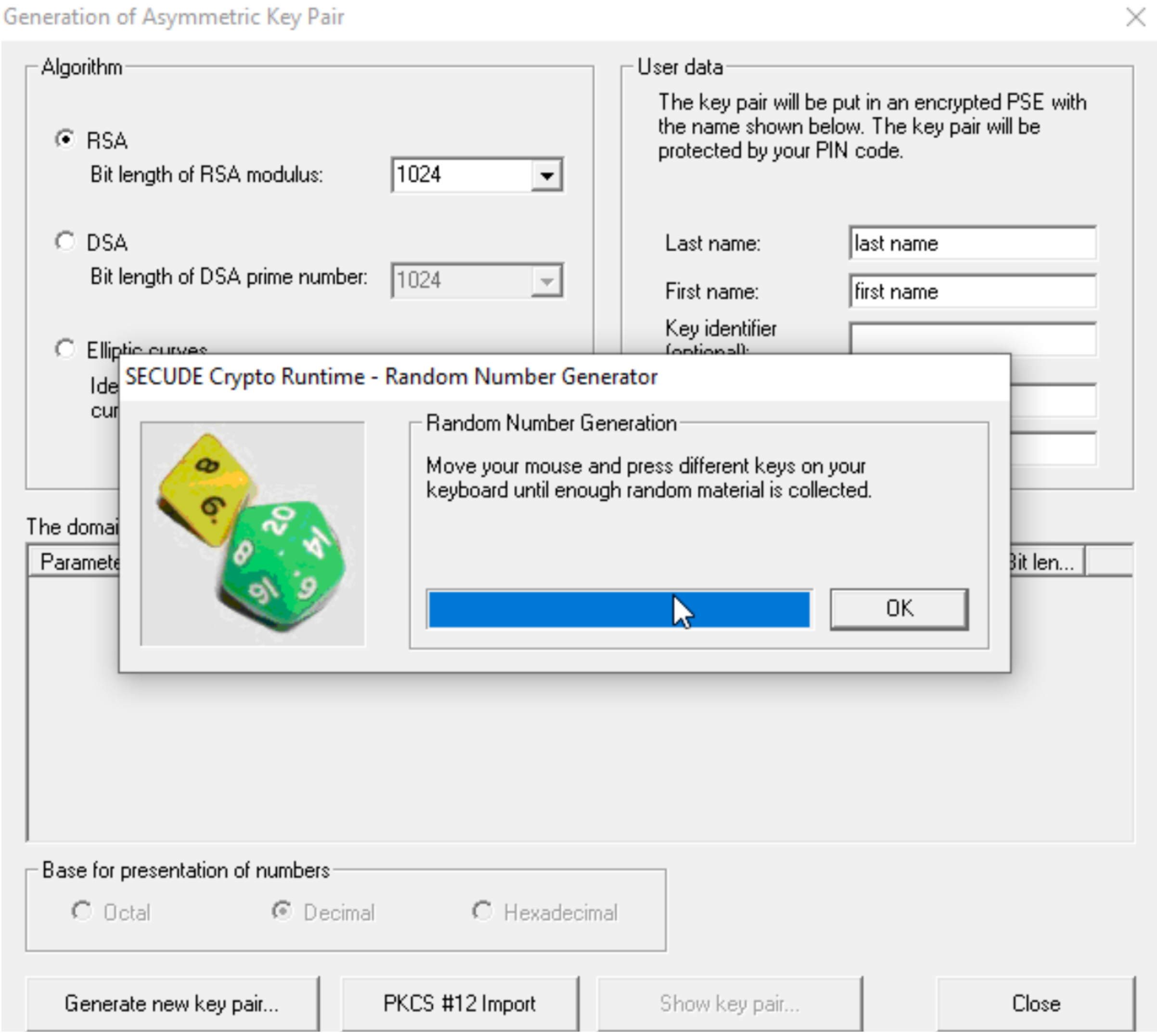

Figure 10: RSA asymmetric key pair generation.

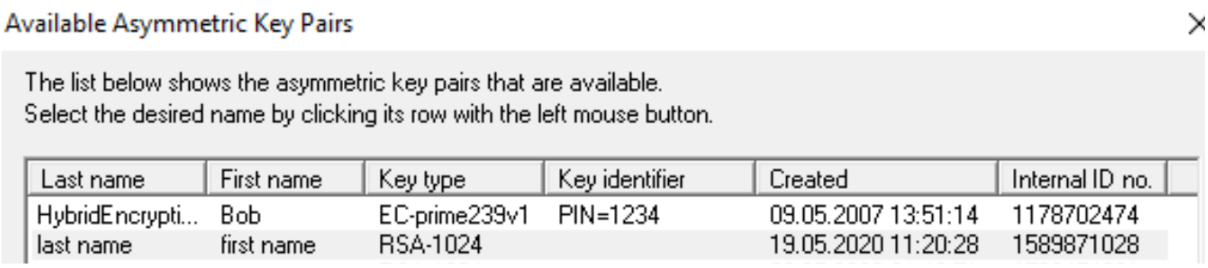

Figure 11: generated key pair

4.

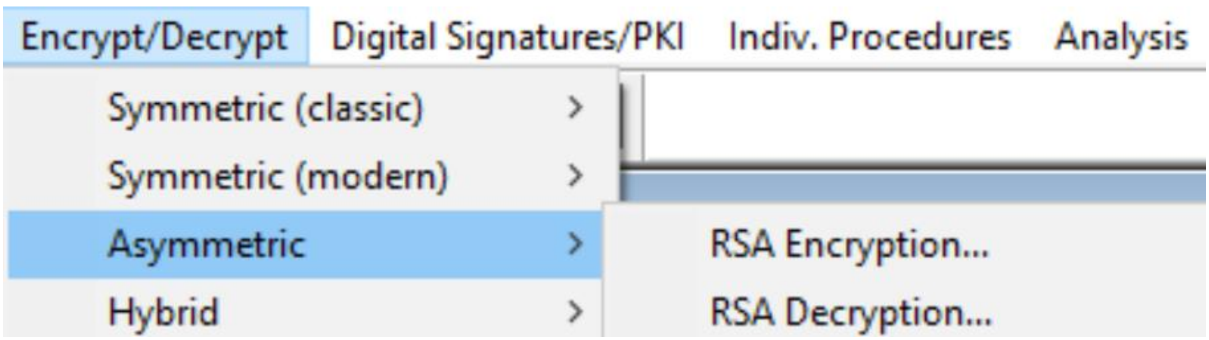

Figure 12: RSA encryption/decryption tool

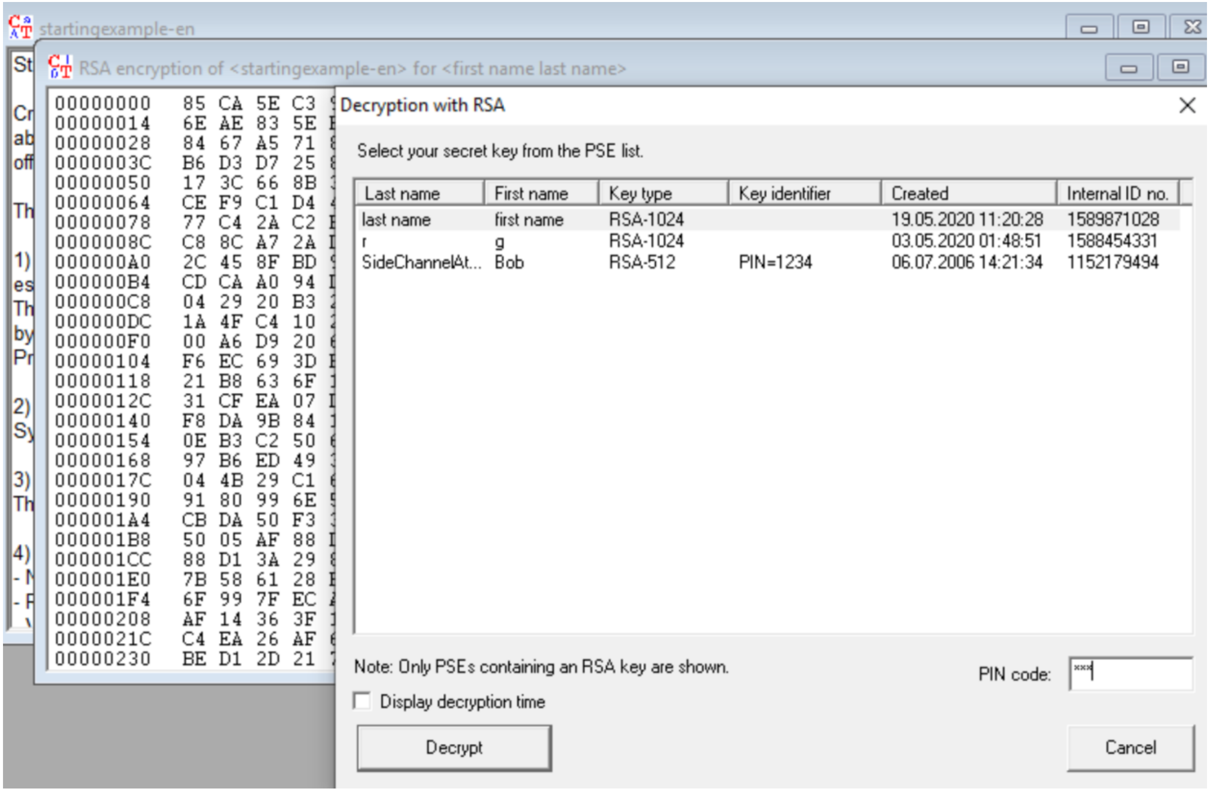

Figure 13: first, encrypting and then, decrypting a chosen text using our generated key

Programming

Two files have been attached for this section.

Optional Question

8. Proof the problems of decrypting arbitrary ElGamal ciphertext mod p and breaking arbitrary Diffie-Hellman mod p are equivalent.

حل :

باید یک الگوریتم داشته باشیم که بتواند متن رمز شده (r,t) دلخواه الجمال را با کلید عمومی مربوطه (p,a,b) رمزگشایی کند تا پیام $m = t.r^{-log_a b}\ (mod\ p)$ را تولید کند. ما هدفمان شکست مساله دیفی هلمن هست که مقدار $g^{xy}(mod\ p)$ را با مقادیر داده شده (p,g,c_x,c_y) که مقادیرش برابر $c_x = g^x(mod\ p)$ و $c_y = g^y(mod\ p)$ است محاسبه کند. برای انجام این، الگوریتم الجمال مقادیر (p,a,b,r,t) را با $a = g, b = c_x, t = 1, r = c_y$ می دهد. پیام خروجی به این شکل می‌شود. $m = 1\,.(g^y)^{-log_g(g^x)} \equiv g^{-xy}\ (mod\ p)$ در نتیجه $g^{xy} \equiv m^{-1}\ (mod\ p)$ می تواند محاسبه شود.

متقابلا، فرض می‌کنیم الگوریتمی داشته باشیم که بتواند مساله دیفی هلمن محاسبه مقدار $g^{xy}\ (mod\ p)$ را بشکند و مقدار (p,g,c_x,c_y) را که $c_x = g^x(mod\ p)$ و $c_y = g^y(mod\ p)$ است به ما بدهد. ما

می‌خواهیم متن رمز شده الجمال (r,t) را با کلید عمومی مربوطه (p,a,b) رمزگشایی کنیم تا پیام $m = t.r^{-log_a b}\ (mod\ p)$ را بدست آوریم. برای انجام این کار، الگوریتم دیفی هلمن مقدار (p,g,c_x,c_y) را که $g = a\ , c_x = b, c_y = r$ است به ما می دهد. این به ما مقدار خروجی ${c_x}^{log_g c_y} = b^{log_a r} = b^k$ را می دهد. در نتیجه مقدار $m \equiv t.b^{-k}\ (mod\ p)$ را حساب می کنیم.