۱.

۱.۱.

$$k_{pr} = 1 \;\; \Rightarrow \;\; k_{pub} = \alpha^1 \;\; mod \; p = \alpha$$
$$k_{pr} = p - 1 \;\; \Rightarrow \;\; k_{pub} = \alpha^{p-1} \;\; mod \; p = 1$$

بنابراین کلیدهای $p - 1$ و 1 ، یک کلید ضعیف به حساب می‌آیند و در صورتی که مورد استفاده قرار بگیرند؛ مهاجم به راحتی می‌تواند مقدار کلید خصوصی را بدست آورد.

۲.۱.

باید یک الگوریتم داشته باشیم که بتواند متن رمزشده (k_E, y) دلخواه الجمال با کلید عمومی $k_{pub} = (p, \alpha, \beta)$ را رمزگشایی کند تا پیام $m = y \cdot k_E^{-\log_\alpha \beta} \;\; mod \; p$ بدست آید. هدف ما شکستن مسئله دیفی هلمن است که مقدار $\alpha^{ab} \;\; mod \; p$ را با پارامترهای $k_{pub} = (p, \alpha, A, B)$ محاسبه کند. بنابراین با استفاده از الگوریتم الجمال داریم:

$$y = 1 \;\; , \;\; k_E = B \;\; , \;\; \beta = A \quad \Rightarrow \quad m = 1 \cdot B^{-\log_\alpha A} \;\; mod \; p$$

متقابلاً فرض می‌کنیم الگوریتمی داشته باشیم که بتواند مسئله دیفی هلمن با پارامترهای $k_{pub} = (p, \alpha, A, B)$ بشکند و مقدار $\alpha^{ab} \;\; mod \; p$ را محاسبه کند. در این‌جا می‌خواهیم متن رمزشده الجمال (k_E, y) با کلید عمومی $k_{pub} = (p, \alpha, \beta)$ را رمز گشایی کند. بنابراین با استفاده از دیفی هلمن داریم:

$$B = k_E \;\; , \;\; A = \beta \quad \Rightarrow \quad \alpha^{ab} = A^{\log_\alpha B} = \beta^{\log_\alpha k_E} = \beta^i \;\; mod \; p$$
$$\Rightarrow \quad m = y \cdot \beta^{-i} \;\; mod \; p$$

۲.

منظور از primitive root یا مولد یک عدد p عددی مانند α است به‌طوری که باقی‌مانده همه‌ی توان‌های α به پیمانه‌ی p همه‌ی اعداد 1 تا $p - 1$ را شامل گردد.

- با توجه به این‌که اعداد داده شده به فرم p^k و $2p^k$ هستند، که p یک عدد اول فرد و $k \geq 1$ است؛ بنابراین همه‌ی آن‌ها دارای مولد می‌باشند.
- عنصر $\alpha \in Z_n^*$ یک مولد گروه Z_n^* است، اگر و تنها اگر $\alpha^{\Phi(n)/p} \neq 1 \;\; mod \; n$ که مقدار p یک عامل اول $\Phi(n)$ می‌باشد.

اگر مقدار $\alpha = 2$ در نظر بگیریم، باید نشان دهیم که α یک مولد است، بنابراین داریم:

$$if\ \alpha = 2\ ,n = 11 \quad \Rightarrow \quad \Phi(11) = 10 = 2 \times 5 \quad \Rightarrow \quad p = 2{,}5$$

$$p = 2 \quad \Rightarrow \quad \alpha^2 = 2^2\ mod\ 11 = 4\ \neq 1\ mod\ 11$$

$$p = 5 \quad \Rightarrow \quad \alpha^2 = 2^5\ mod\ 11 = 10\ \neq 1\ mod\ 11$$

بنابراین $\alpha = 2$ یک مولد گروه Z_{11}^* است.

$$if\ \alpha = 2\ ,n = 11^2 \quad \Rightarrow \quad \Phi(11^2) = 110 = 2 \times 5 \times 11 \quad \Rightarrow \quad p = 2{,}5{,}11$$

$$p = 2 \quad \Rightarrow \quad \alpha^2 = 2^2\ mod\ 11^2 = 4\ \neq 1\ mod\ 11^2$$

$$p = 5 \quad \Rightarrow \quad \alpha^2 = 2^5\ mod\ 11^2 = 32\ \neq 1\ mod\ 11^2$$

$$p = 11 \quad \Rightarrow \quad \alpha^2 = 2^{11}\ mod\ 11^2 = 112\ \neq 1\ mod\ 11^2$$

بنابراین $\alpha = 2$ یک مولد گروه $Z_{11^2}^*$ است.

$$if\ \alpha = 2\ ,n = 2 \cdot 11^2 \quad \Rightarrow \quad \Phi(2 \cdot 11^2) = 110 = 2 \times 5 \times 11 \quad \Rightarrow \quad p = 2{,}5{,}11$$

$$p = 2 \quad \Rightarrow \quad \alpha^2 = 2^2\ mod\ 2 \cdot 11^2 = 4\ \neq 1\ mod\ 2 \cdot 11^2$$

$$p = 5 \quad \Rightarrow \quad \alpha^2 = 2^5\ mod\ 2 \cdot 11^2 = 32\ \neq 1\ mod\ 2 \cdot 11^2$$

$$p = 11 \quad \Rightarrow \quad \alpha^2 = 2^{11}\ mod\ 2 \cdot 11^2 = 112\ \neq 1\ mod\ 2 \cdot 11^2$$

بنابراین $\alpha = 2$ یک مولد گروه $Z_{2 \cdot 11^2}^*$ است.

$$if\ \alpha = 2\ ,n = 11^{100} \quad \Rightarrow \quad \Phi(11^{100}) = 2 \times 5 \times 11^{99} \quad \Rightarrow \quad p = 2{,}5{,}11$$

$$p = 2 \quad \Rightarrow \quad \alpha^2 = 2^2\ mod\ 11^{100} = 4\ \neq 1\ mod\ 11^{100}$$

$$p = 5 \quad \Rightarrow \quad \alpha^2 = 2^5\ mod\ 11^{100} = 32\ \neq 1\ mod\ 11^{100}$$

$$p = 11 \quad \Rightarrow \quad \alpha^2 = 2^{11}\ mod\ 11^{100} = 2048\ \neq 1\ mod\ 11^{100}$$

بنابراین $\alpha = 2$ یک مولد گروه $Z_{11^{100}}^*$ است.

بنابراین $\alpha = 2$ یک مولد برای اعداد 11 ، 11^2 ، $2 \cdot 11^2$ و 11^{100} است.

۳.

ابتدا کلید عمومی باب را محاسبه می‌کنیم:

$$\beta = \alpha^d\ mod\ p = 7^{22105}\ mod\ 44927 = 40909$$

$$\Rightarrow \quad k_{pub} = (p, \alpha, \beta) = (44927, 7, 40909)$$

برای رمز کردن متن، یک i تصادفی در محدوده $2 \le i \le p-2$ انتخاب می‌کنیم، سپس داریم:

$$i = 67 \quad \Rightarrow \quad k_E = \alpha^i \ mod\ p = 7^{67} \ mod\ 44927 = 38737$$

$$\Rightarrow \quad k_M = \beta^i \ mod\ p = 40909^{67} \ mod\ 44927 = 25566$$

$$\Rightarrow \quad y = m \cdot k_M \ mod\ p = 10101 \cdot 25566 \ \ mod\ 44927 = 1770$$

بنابراین آلیس متن رمز شده $(k_E, y) = (38737, 1770)$ را برای باب می‌فرستد.

باب برای رمزگشایی متن رمزشده عملیات زیر را انجام می‌دهد:

$$k_M = k_E^d \ mod\ p = 38737^{22105} \ mod\ 44927 = 25566$$

$$\Rightarrow \quad m = y \cdot k_M^{-1} \ mod\ p = 1770 \cdot 25566^{-1} \ mod\ 44927 = 10101$$

.۴

.۱.۴

$$y^2 = x^3 + 2x + 2 \quad mod\ 17 \quad \Rightarrow \quad a = 2\,, \ b = 2\,, \ p = 17$$

$$4a^3 + 27b^2 = 4 \times 2^3 + 27 \times 2^2 = 140 \ \ mod\ 17 = 4 \neq 0 \quad mod\ 17$$

.۲.۴

$$(2,7) + (5,2) \ \Rightarrow \ \ x_1 = 2\,, \ x_2 = 5\,, \ y_1 = 7\,, \ y_2 = 2$$

$$s = (y_1 - y_2)(x_2 - x_1)^{-1} \ mod\ 17$$

$$\Rightarrow \ s = (7-2)(5-2)^{-1} \ mod\ 17 = (-5)(3)^{-1} \ mod\ 17$$

$$\Rightarrow \ s = (-5)(6) = -30 = 4 \ \ mod\ 17$$

$$\Rightarrow \quad x_3 = s^2 - x_1 - x_2 \ \ mod\ 17 = 4^2 - 2 - 5 \quad mod\ 17 \ = 9$$

$$\Rightarrow \quad y_3 = s(x_1 - x_3) - y_1 \ mod\ 17 = 4(2-9) - 7 \ \ mod\ 17 = 16$$

$$\Rightarrow \quad (x_3, y_3) = (2,7) + (5,2) = (9,16)$$

.۳.۴

$$Hesse's\ Theorem: \quad p + 1 - 2\sqrt{p} \le \#E \le p + 1 + 2\sqrt{p}$$

$$\#E = 19, \ \ p = 17 \quad \Rightarrow \quad 17 + 1 - 2\sqrt{17} \le 19 \le 17 + 1 + 2\sqrt{17}$$

$$\Rightarrow \quad 9.75 \le 19 \le 26.24$$

۴.۴.

طبق قضیه ۸.۲.۴ کتاب درسی، با توجه به این‌که تعداد نقاط بر روی این خم که تشکیل یک گروه دوری محدود می‌دهند، عددی اول است، بنابراین تمامی عناصر این گروه primitive elements می‌باشند.

۵.

۱.۵.

$$x = 0 \quad \Rightarrow \quad y^2 = 0^3 + 3 \cdot 0 + 2 = 2 \quad mod\ 7 \quad \Rightarrow \quad y = 3,4$$

$$x = 1 \quad \Rightarrow \quad y^2 = 1^3 + 3 \cdot 1 + 2 = 6 \quad mod\ 7 \Rightarrow \quad \text{جواب ندارد}$$

$$x = 2 \quad \Rightarrow \quad y^2 = 2^3 + 3 \cdot 2 + 2 = 2 \quad mod\ 7 \quad \Rightarrow \quad y = 3,4$$

$$x = 3 \quad \Rightarrow \quad y^2 = 3^3 + 3 \cdot 3 + 2 = 3 \quad mod\ 7 \Rightarrow \quad \text{جواب ندارد}$$

$$x = 4 \quad \Rightarrow \quad y^2 = 4^3 + 3 \cdot 4 + 2 = 1 \quad mod\ 7 \quad \Rightarrow \quad y = 1,6$$

$$x = 5 \quad \Rightarrow \quad y^2 = 5^3 + 3 \cdot 5 + 2 = 2 \quad mod\ 7 \quad \Rightarrow \quad y = 3,4$$

$$x = 6 \quad \Rightarrow \quad y^2 = 6^3 + 3 \cdot 6 + 2 = 5 \quad mod\ 7 \Rightarrow \quad \text{جواب ندارد}$$

بنابراین نقاط این منحنی برابر است با:

$$\{(0,3)\ , (0,4)\ , (2,3)\ , (2,4)\ , (4,1)\ , (4,6)\ , (5,3)\ , (5,4)\}$$

۲.۵.

مرتبه گروه برابر است با:

$$\#E\ = \#\{O\ , (0,3)\ , (0,4)\ , (2,3)\ , (2,4)\ , (4,1)\ , (4,6)\ , (5,3)\ , (5,4)\} = 9$$

۳.۵.

$$0 \cdot \alpha = O \quad , \quad 1 \cdot \alpha = (0,3) \quad , \quad 2 \cdot \alpha = (2,3) \quad , \quad 3 \cdot \alpha = (5,4)$$

$$4 \cdot \alpha = (4,6) \quad , \quad 5 \cdot \alpha = (4,1) \quad , \quad 6 \cdot \alpha = (5,3) \quad , \quad 7 \cdot \alpha = (2,4)$$

$$8 \cdot \alpha = (0,4) \quad , \quad 9 \cdot \alpha = O = 0 \cdot \alpha$$

$$\Rightarrow \quad ord(\alpha) = 9 = \#E \quad \Rightarrow \quad \boldsymbol{\alpha}\ \ is\ primitive\ element$$

۶.

$$k_{pr} = a = 6\,,\;\; k_{pub} = B = (5{,}9) \quad \Rightarrow \quad K = aB = 6 \cdot B = 2(2B + B)$$

$$2B = (x_3, y_3):\;\; x_1 = x_2 = 5\,,\;\; y_1 = y_2 = 9$$

$$s = (3x_1^2 + a) \cdot 2{y_1}^{-1} \;\; mod\ 11 = \; (3 \cdot 5^2 + 1)(2 \cdot 9)^{-1} \;\; mod\ 11 = 3$$

$$x_3 = s^2 - x_1 - x_2 \;\; mod\ 11 = 3^2 - 5 - 5 \quad mod\ 11 \; = 10$$

$$y_3 = s(x_1 - x_3) - y_1 \;\; mod\ 11 = 3(5 - 10) - 9 \;\; mod\ 11 = 9$$

$$\Rightarrow \quad 2B = (x_3, y_3) = (10{,}9)$$

$$3B = 2B + B = (x_3', y_3'):\;\; x_1 = 10\,, x_2 = 5\,,\;\; y_1 = y_2 = 9$$

$$s = (y_1 - y_2)(x_2 - x_1)^{-1} \;\; mod\ 11 = \; (9 - 9)(5 - 10)^{-1} \;\; mod\ 11 = 0$$

$$x_3' = s^2 - x_1 - x_2 \;\; mod\ 11 = 0^2 - 10 - 5 \quad mod\ 11 \; = 7$$

$$y_3' = s(x_1 - x_3') - y_1 \;\; mod\ 11 = 0(5 - 7) - 9 \;\; mod\ 11 = 2$$

$$\Rightarrow \quad 3B = (x_3', y_3') = (7{,}2)$$

$$6B = 2 \cdot 3B = (x_3'', y_3''):\;\; x_1 = x_2 = 7\,,\;\; y_1 = y_2 = 2$$

$$s = (3x_1^2 + a) \cdot 2{y_1}^{-1} \;\; mod\ 11 = \; (3 \cdot 7^2 + 1)(2 \cdot 2)^{-1} \;\; mod\ 11 = 4$$

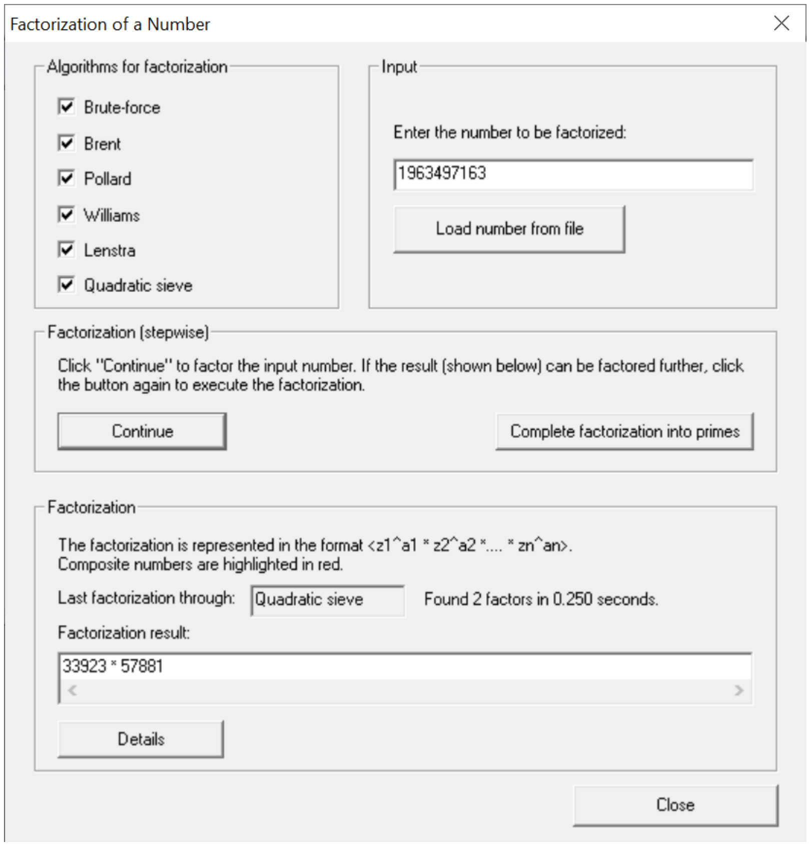
$$x_3'' = s^2 - x_1 - x_2 \;\; mod\ 11 = 4^2 - 7 - 7 \quad mod\ 11 \; = 2$$

$$y_3'' = s(x_1 - x_3'') - y_1 \;\; mod\ 11 = 4(7 - 2) - 2 \;\; mod\ 11 = 7$$

$$\Rightarrow \quad 6B = (x_3'', y_3'') = (2{,}7)$$

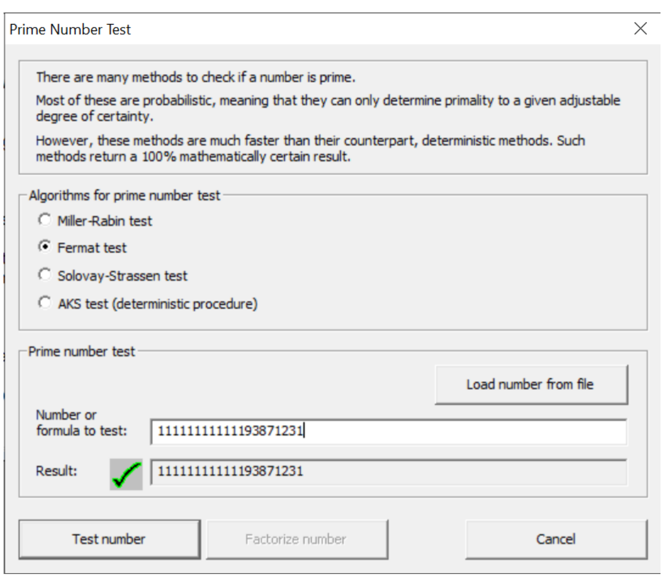
$$\Rightarrow \quad K_{AB} = x_3'' = 2$$

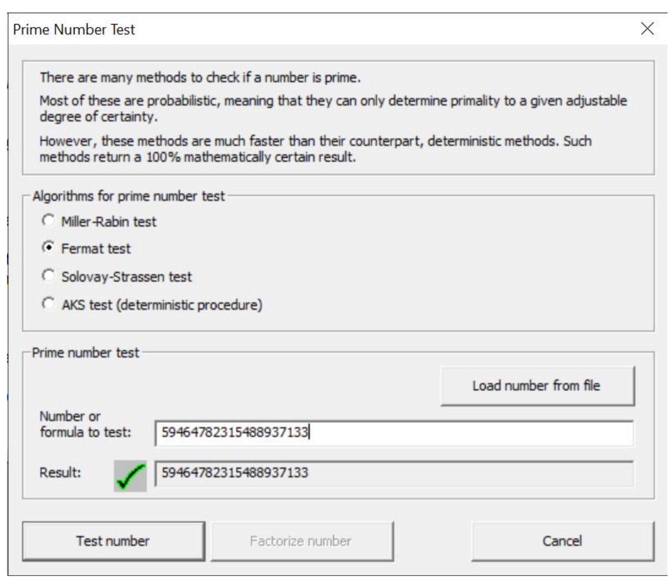
7.

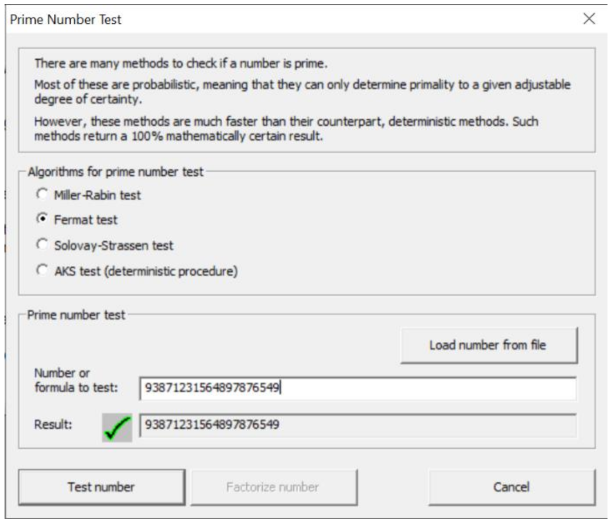


8.

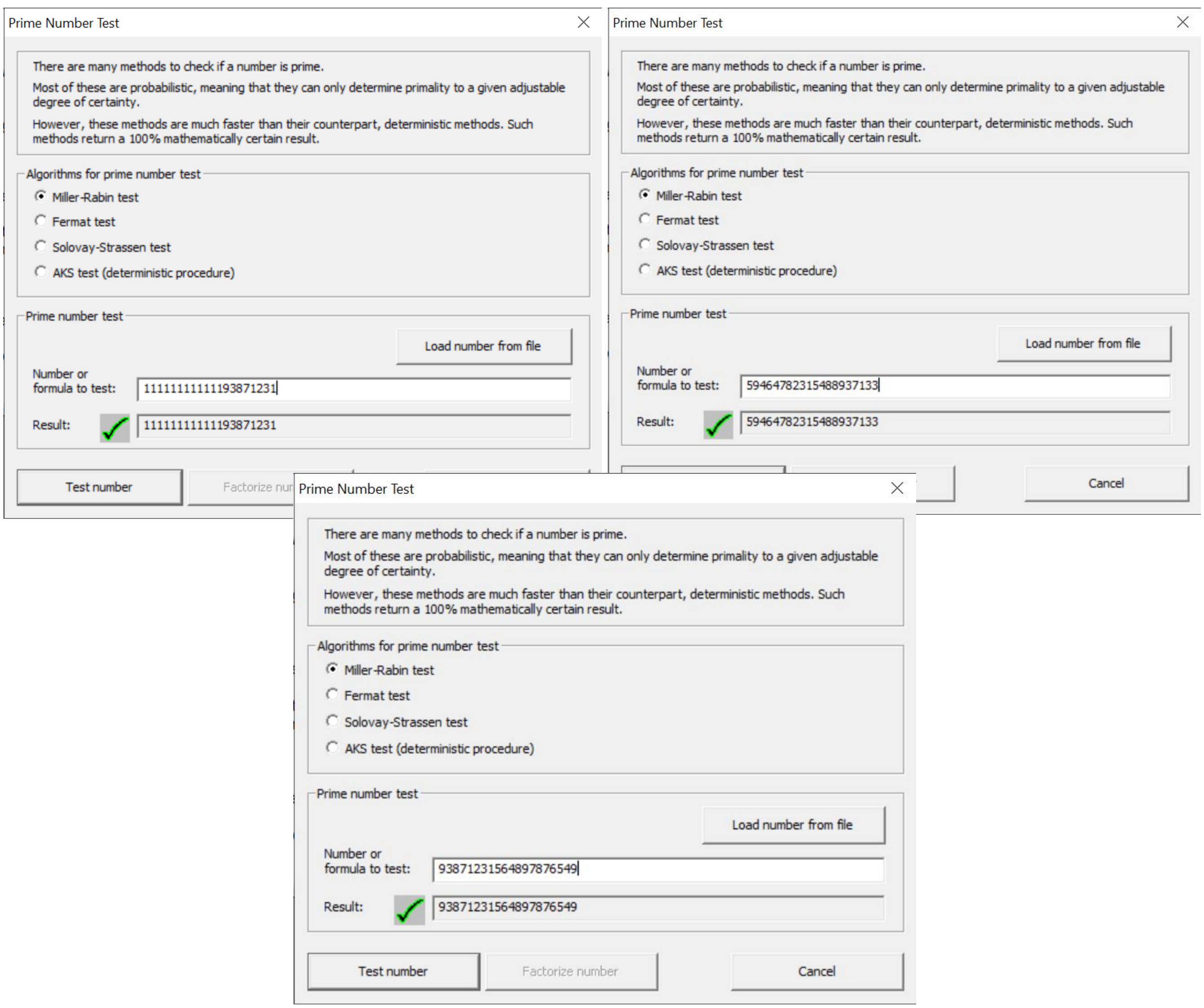
a. large prime number, Fermat test



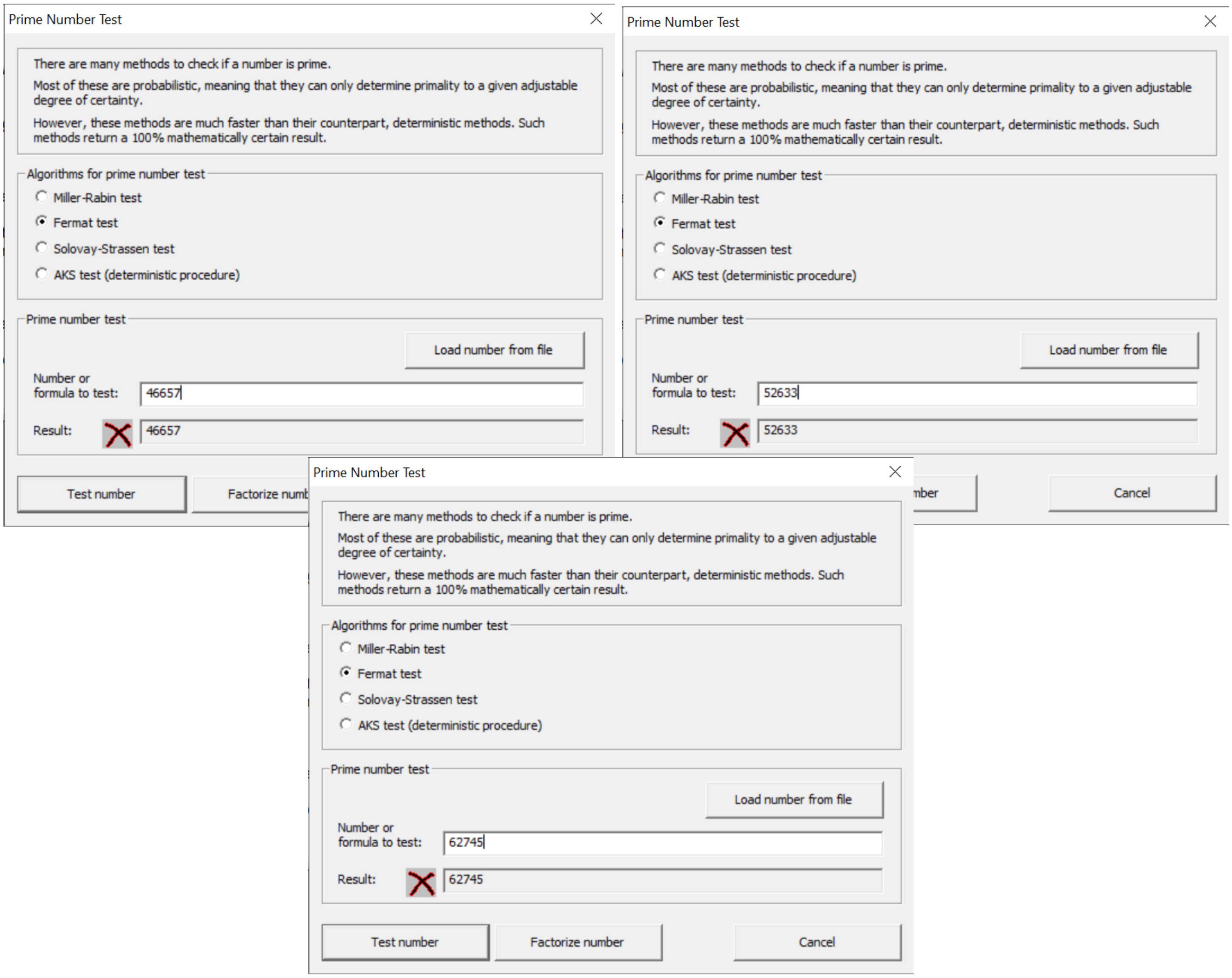




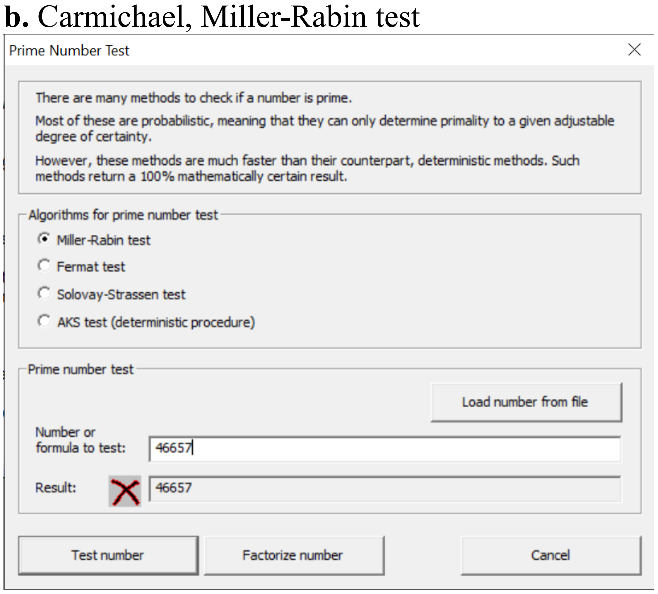
b. large prime number, Miller-Rabin test

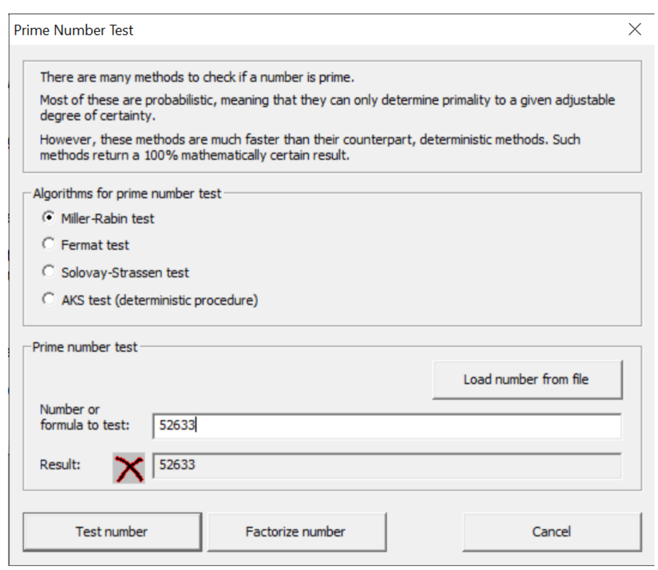


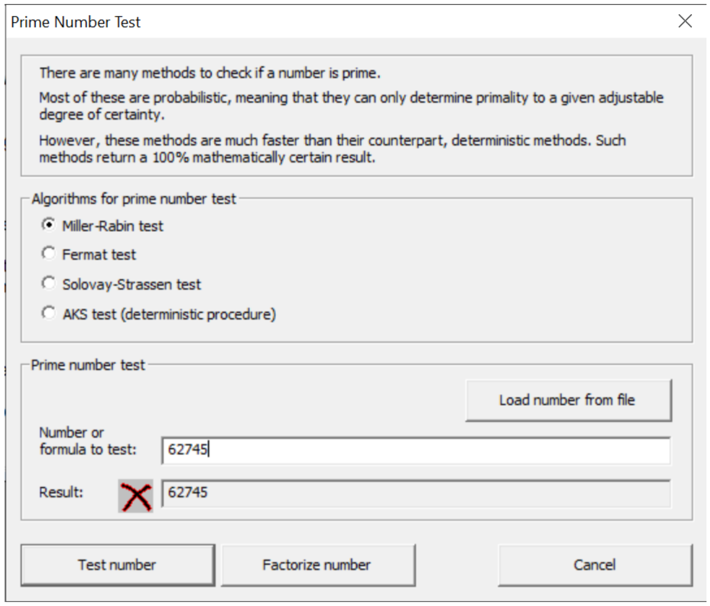
a. Carmichael, Fermat test



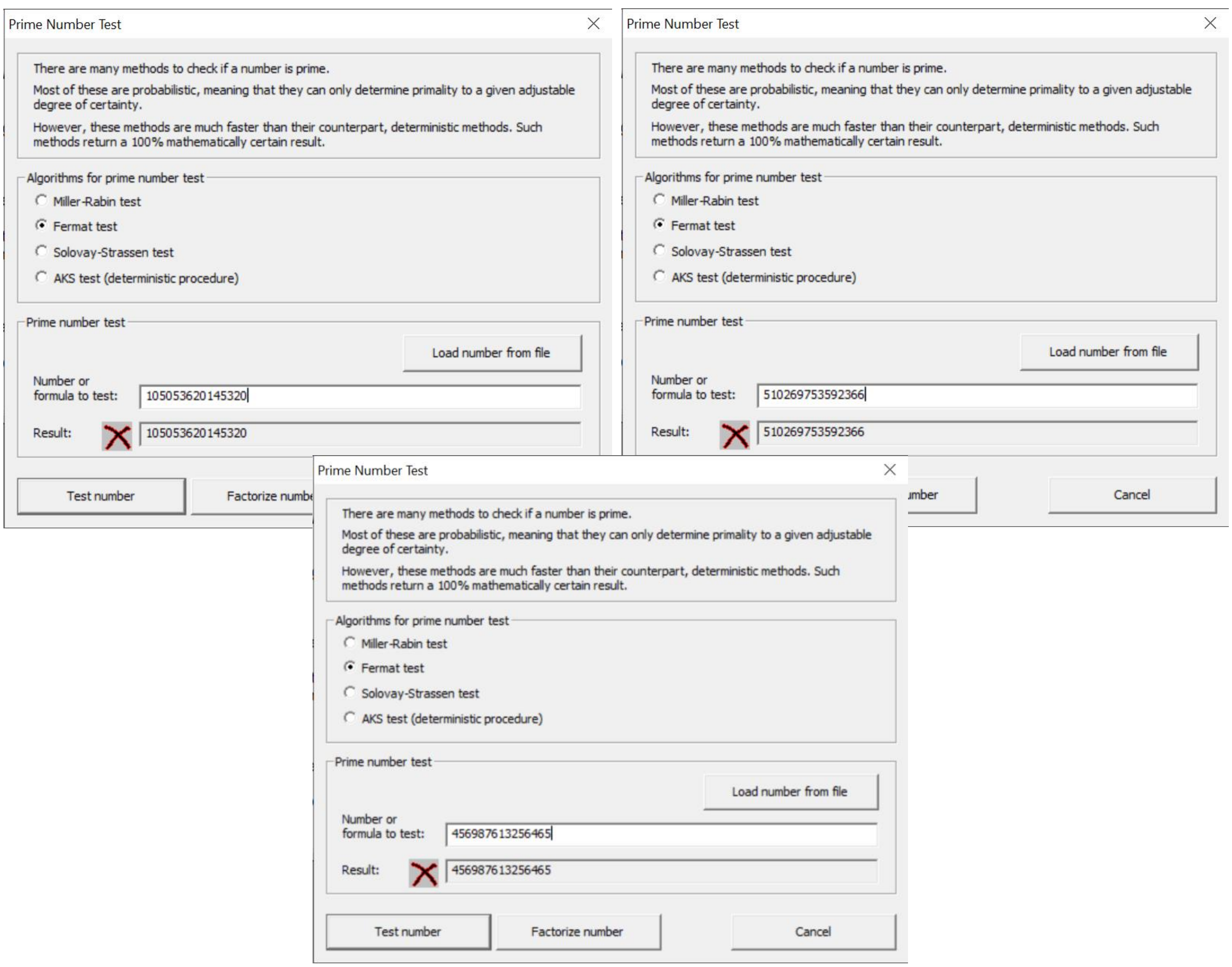
b. Carmichael, Miller-Rabin test



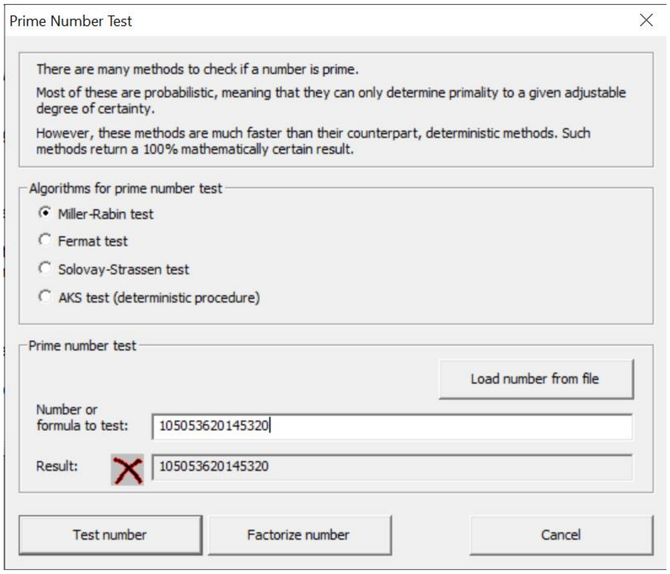


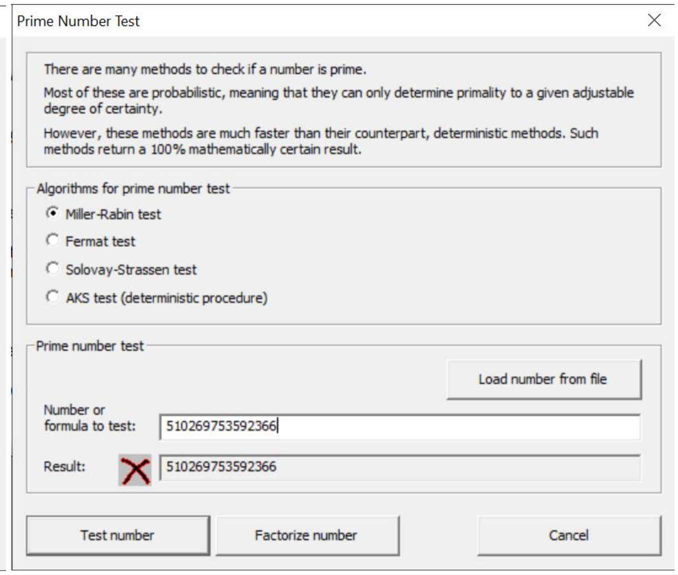


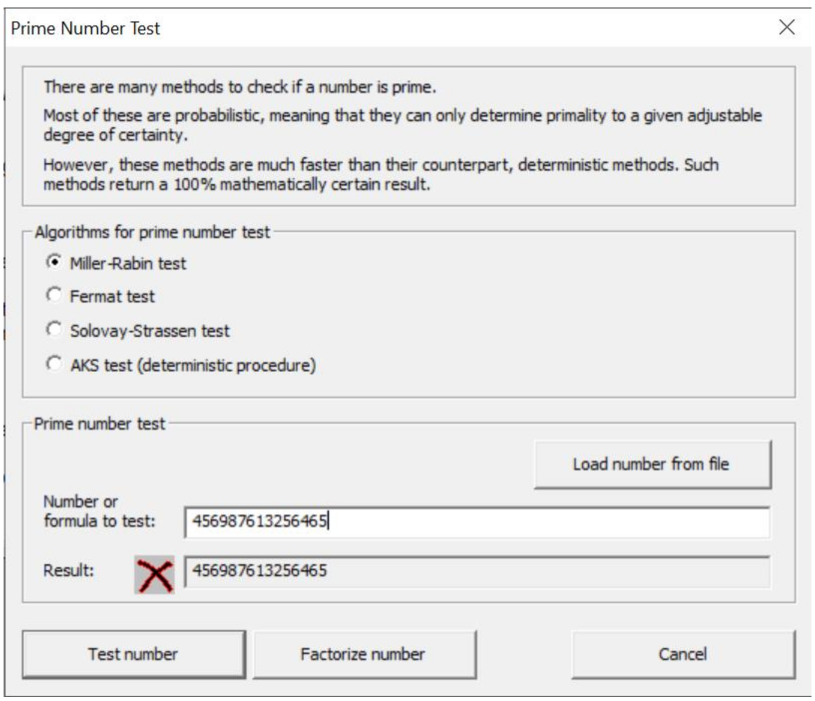
a. Composite number, Fermat test



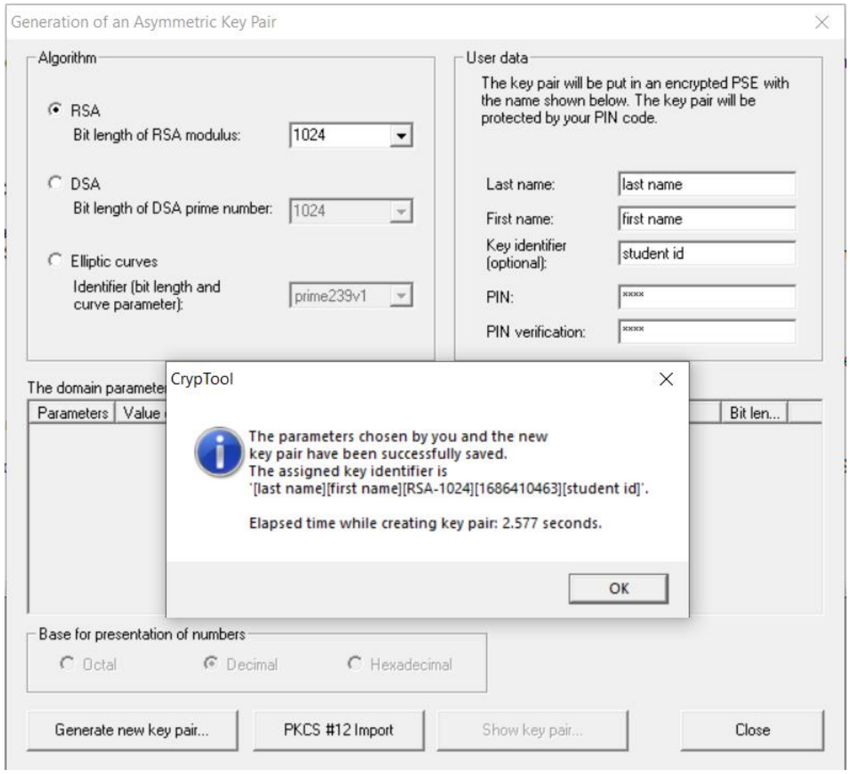
b. Composite number, Miller-Rabin test

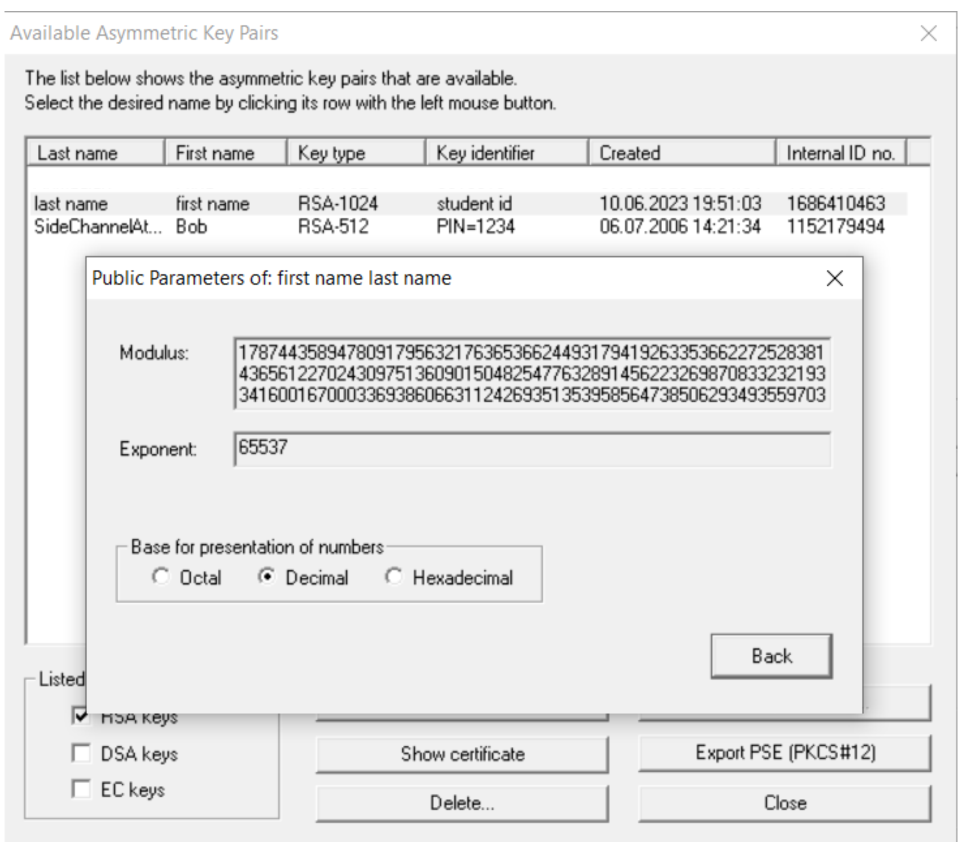






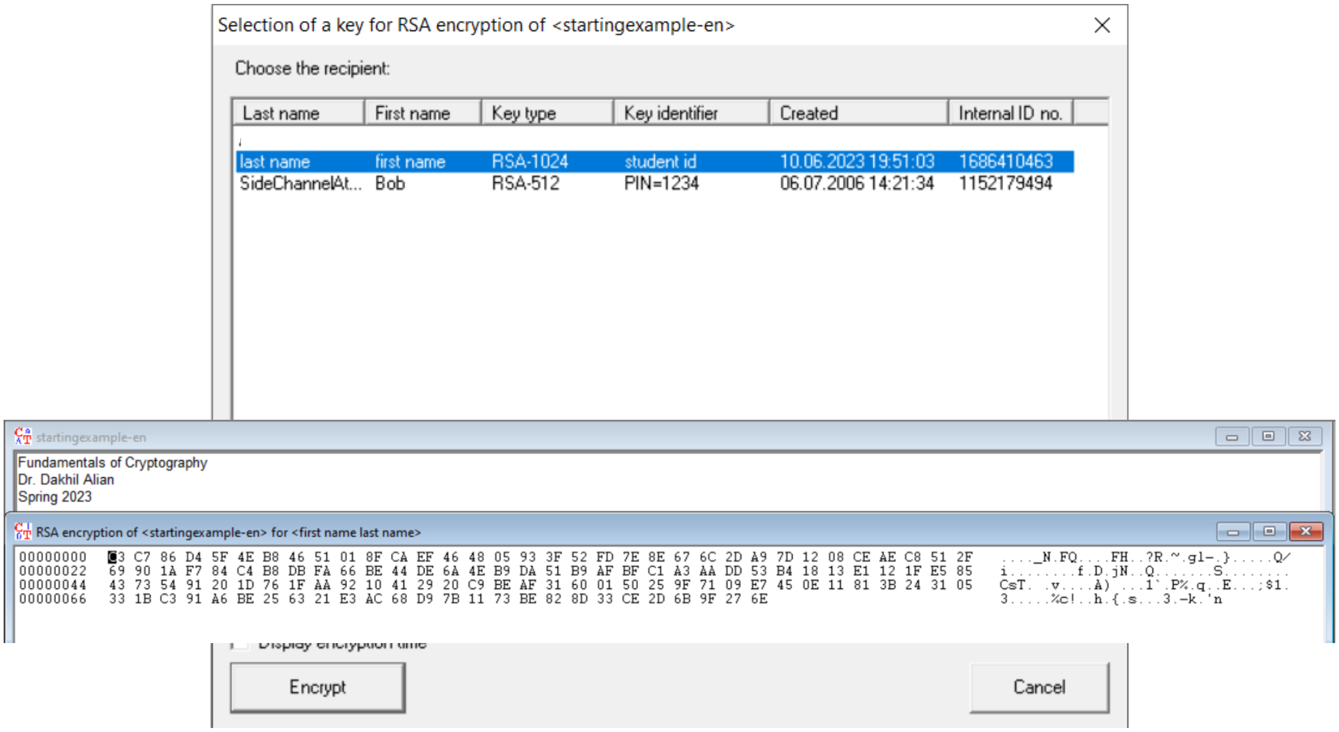
9.


Generation of an Asymmetric Key Pair
Algorithm
RSA
Bit length of RSA modulus:
1024
DSA
Bit length of DSA prime number:
1024
Elliptic curves
Identifier (bit length and curve parameter):
prime239v1
User data
The key pair will be put in an encrypted PSE with the name shown below. The key pair will be protected by your PIN code.
Last name:
last name
First name:
first name
Key identifier (optional):
student id
PIN:
PIN verification:
The domain paramete
Parameters
Value
Bit len...
CrypTool
The parameters chosen by you and the new key pair have been successfully saved.
The assigned key identifier is
'[last name][first name][RSA-1024][1686410463][student id]'.
Elapsed time while creating key pair: 2.577 seconds.
OK
Base for presentation of numbers
Octal
Decimal
Hexadecimal
Generate new key pair...
PKCS #12 Import
Show key pair...
Close

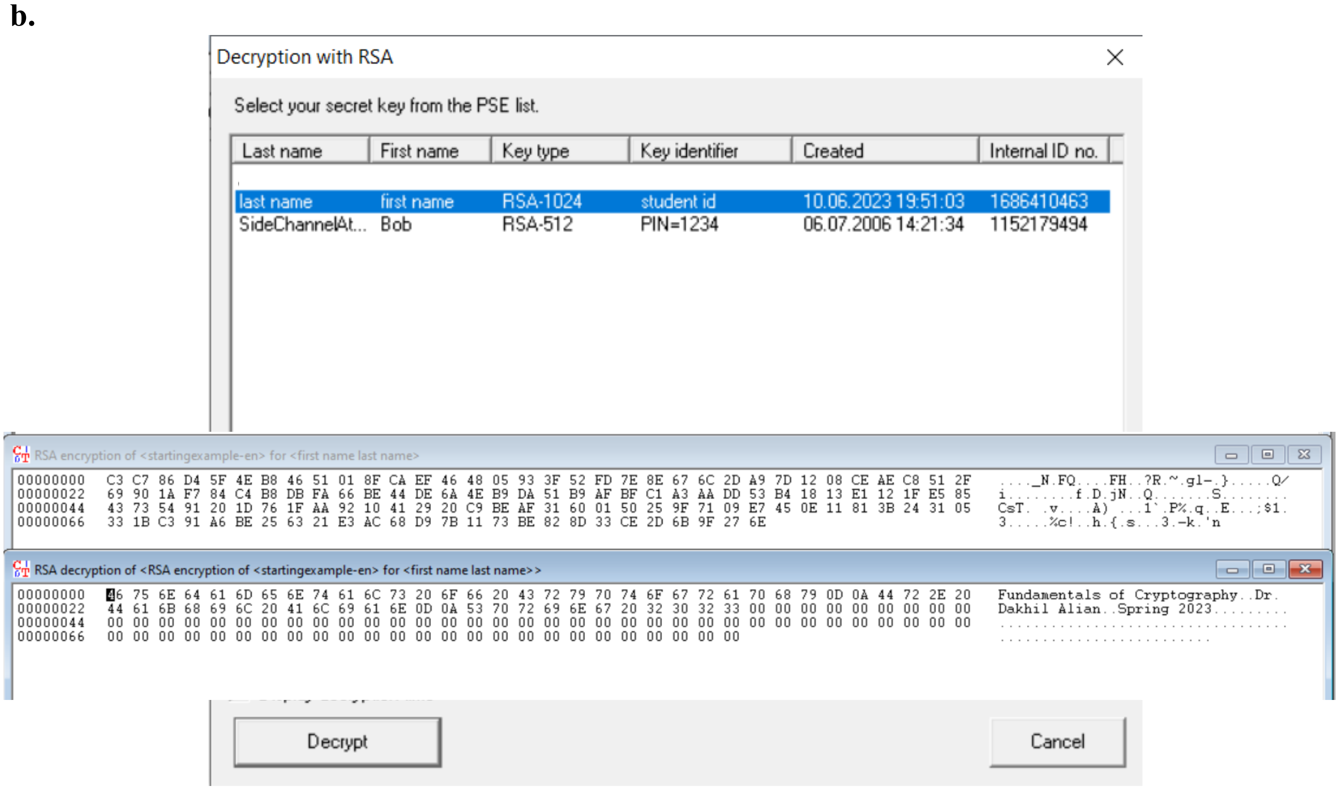

Available Asymmetric Key Pairs
The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.
Last name | First name | Key type | Key identifier | Created | Internal ID no.
last name | first name | RSA-1024 | student id | 10.06.2023 19:51:03 | 1686410463
SideChannelAt... | Bob | RSA-512 | PIN=1234 | 06.07.2006 14:21:34 | 1152179494
Public Parameters of: first name last name
Modulus:
1787443589478091795632176365366244931794192633536622725283814365612270243097513609015048254776328914562232698708332321933416001670003369386066311242693513539585647385062934935597 03
Exponent:
65537
Base for presentation of numbers
Octal
Decimal
Hexadecimal
Back
Listed
RSA keys
DSA keys
EC keys
Show certificate
Export PSE (PKCS#12)
Delete...
Close

10.

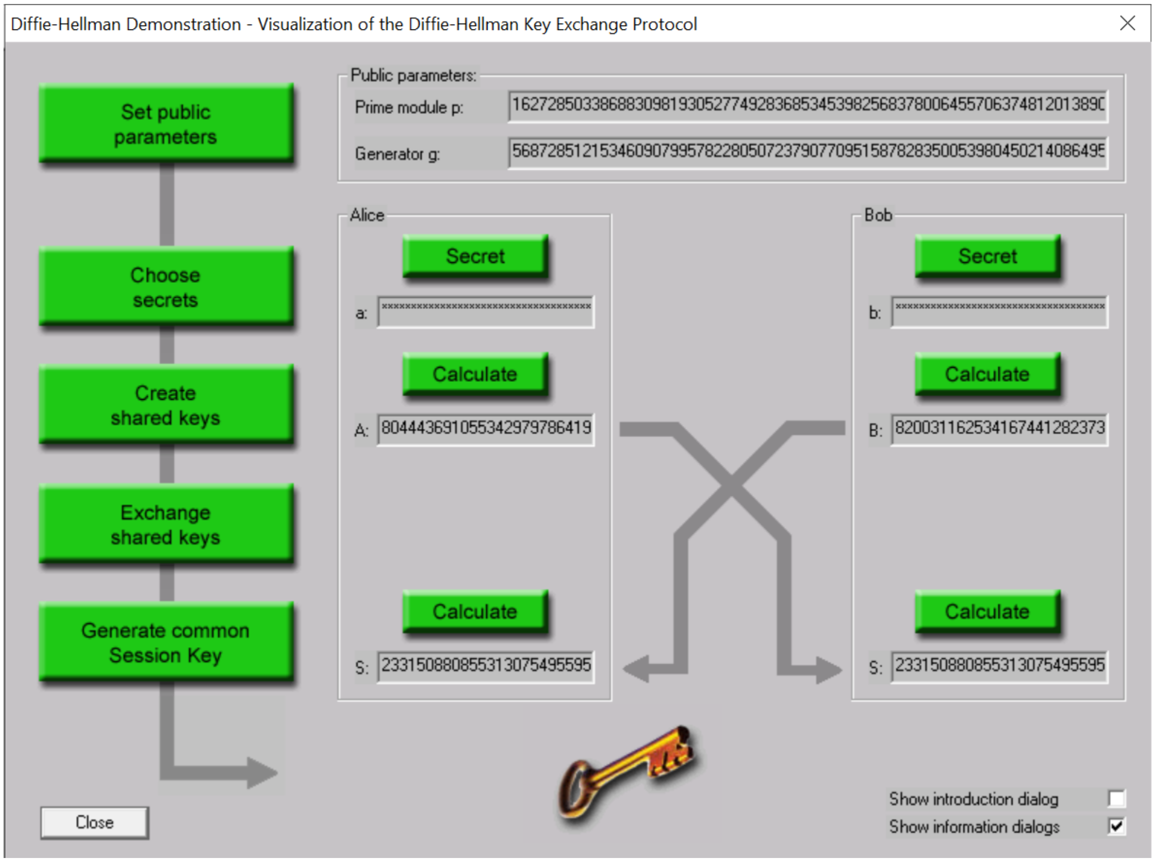
a.


Selection of a key for RSA encryption of <startingexample-en>
Choose the recipient:
Last name | First name | Key type | Key identifier | Created | Internal ID no.
last name | first name | RSA-1024 | student id | 10.06.2023 19:51:03 | 1686410463
SideChannelAt... | Bob | RSA-512 | PIN=1234 | 06.07.2006 14:21:34 | 1152179494
startingexample-en
Fundamentals of Cryptography
Dr. Dakhil Alian
Spring 2023
RSA encryption of <startingexample-en> for <first name last name>
00000000 C3 C7 86 D4 5F 4E B8 46 51 01 8F CA EF 46 48 05 93 3F 52 FD 7E 8E 67 6C 2D A9 7D 12 08 CE AE C8 51 2F
00000022 69 90 1A F7 84 C4 B8 DB FA 66 BE 44 DE 6A 4E B9 DA 51 B9 AF BF C1 A3 AA DD 53 B4 18 13 E1 12 1F E5 85
00000044 43 73 54 91 20 1D 76 1F AA 92 10 41 29 20 C9 BE AF 31 60 01 50 25 9F 71 09 E7 45 0E 11 81 3B 24 31 05
00000066 33 1B C3 91 A6 BE 25 63 21 E3 AC 68 D9 7B 11 73 BE 82 8D 33 CE 2D 6B 9F 27 6E
Encrypt
Cancel

b.


Decryption with RSA
Select your secret key from the PSE list.
Last name | First name | Key type | Key identifier | Created | Internal ID no.
last name | first name | RSA-1024 | student id | 10.06.2023 19:51:03 | 1686410463
SideChannelAt... | Bob | RSA-512 | PIN=1234 | 06.07.2006 14:21:34 | 1152179494
RSA encryption of <startingexample-en> for <first name last name>
00000000 C3 C7 86 D4 5F 4E B8 46 51 01 8F CA EF 46 48 05 93 3F 52 FD 7E 8E 67 6C 2D A9 7D 12 08 CE AE C8 51 2F
00000022 69 90 1A F7 84 C4 B8 DB FA 66 BE 44 DE 6A 4E B9 DA 51 B9 AF BF C1 A3 AA DD 53 B4 18 13 E1 12 1F E5 85
00000044 43 73 54 91 20 1D 76 1F AA 92 10 41 29 20 C9 BE AF 31 60 01 50 25 9F 71 09 E7 45 0E 11 81 3B 24 31 05
00000066 33 1B C3 91 A6 BE 25 63 21 E3 AC 68 D9 7B 11 73 BE 82 8D 33 CE 2D 6B 9F 27 6E
RSA decryption of <RSA encryption of <startingexample-en> for <first name last name>>
00000000 46 75 6E 64 61 6D 65 6E 74 61 6C 73 20 6F 66 20 43 72 79 70 74 6F 67 72 61 70 68 79 0D 0A 44 72 2E 20
00000022 44 61 6B 68 69 6C 20 41 6C 69 61 6E 0D 0A 53 70 72 69 6E 67 20 32 30 32 33 00 00 00 00 00 00 00 00 00
00000044 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000066 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Fundamentals of Cryptography..Dr.
Dakhil Alian..Spring 2023.........
Decrypt
Cancel

11.



Prime module:

162728503386883098193052774928368534539825683780064557063748120138904672906063

Generator:

56872851215346090799578228050723790770951587828350053980450214086495875882510

Alice Secret: (a)

37637671944300859829995673367465474789930479789862230707513283462153523158746

Bob Secret: (b)

157706821585949954400476426715785515018106761344652971448482845270033852301930

Alice Public Key: (A)

27548241414191497732861672386964652759965419813694729804443691055342979786419

Bob Public Key: (B)

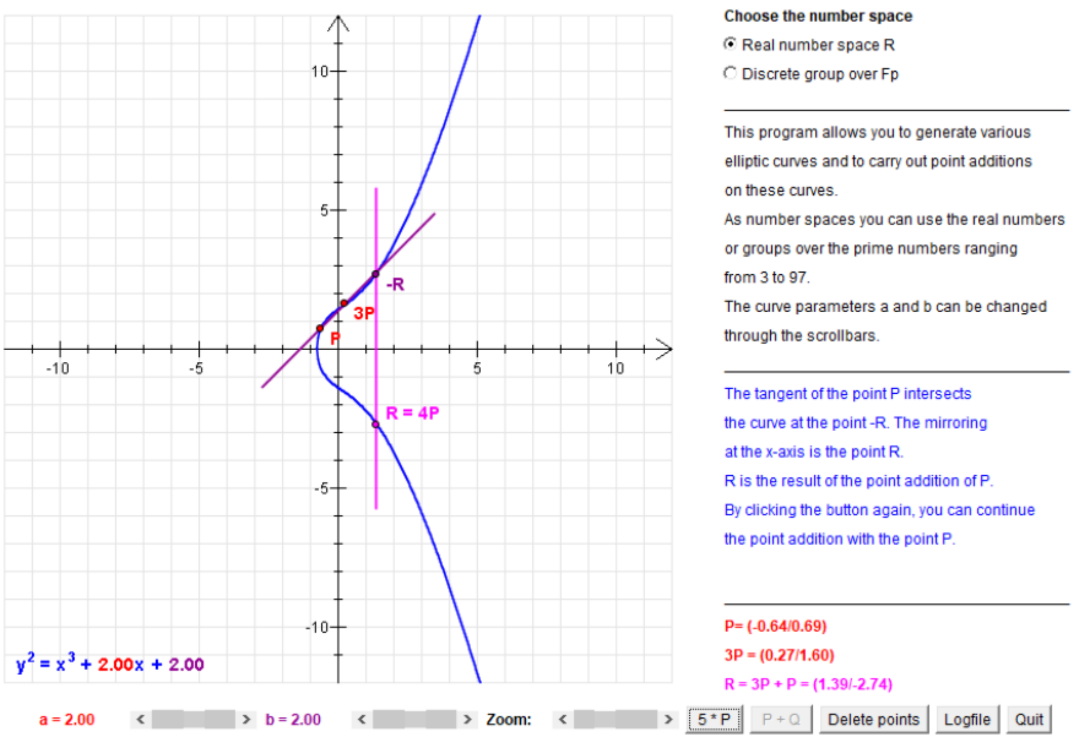
82003116253416744128237353980819441126858185332216109018598249926650912481984

Session Key:

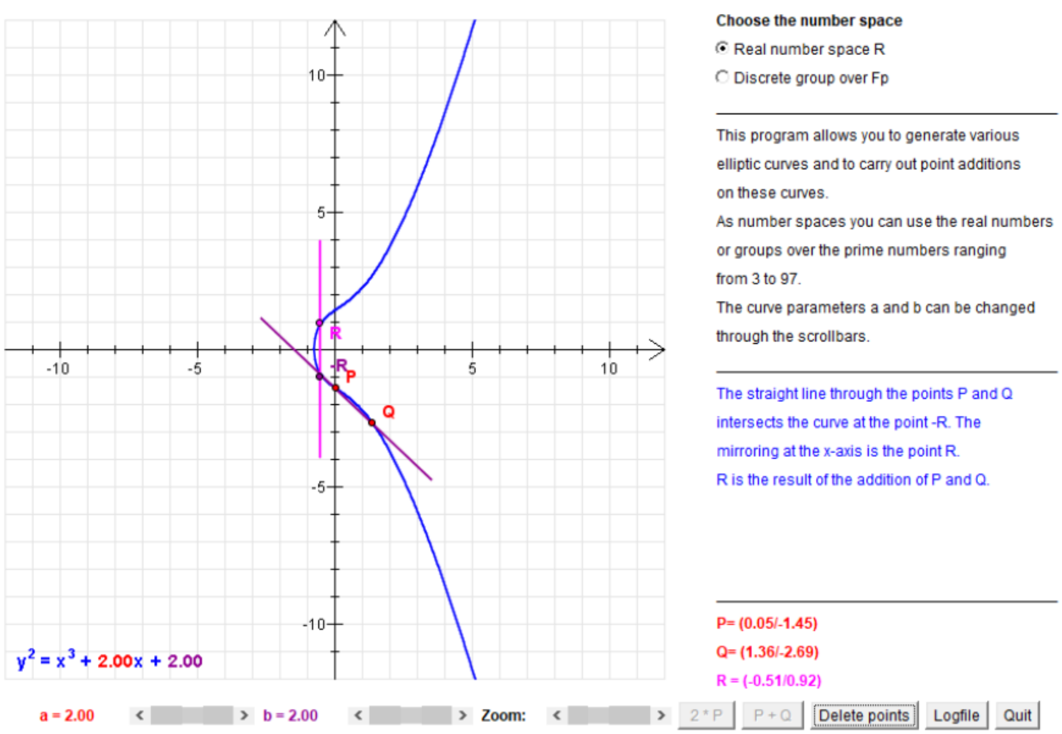
23315088085531307549559511120834977797522759747724190377790412490301979512927

12.

a.


Choose the number space
Real number space R
Discrete group over Fp
This program allows you to generate various elliptic curves and to carry out point additions on these curves.
As number spaces you can use the real numbers or groups over the prime numbers ranging from 3 to 97.
The curve parameters a and b can be changed through the scrollbars.
The tangent of the point P intersects the curve at the point -R. The mirroring at the x-axis is the point R.
R is the result of the point addition of P.
By clicking the button again, you can continue the point addition with the point P.
P= (-0.64/0.69)
3P = (0.27/1.60)
R = 3P + P = (1.39/-2.74)
-R
3P
P
R = 4P
y2 = x3 + 2.00x + 2.00
a = 2.00
b = 2.00
Zoom:
5 * P
P + Q
Delete points
Logfile
Quit

b.


Choose the number space
Real number space R
Discrete group over Fp
This program allows you to generate various elliptic curves and to carry out point additions on these curves.
As number spaces you can use the real numbers or groups over the prime numbers ranging from 3 to 97.
The curve parameters a and b can be changed through the scrollbars.
The straight line through the points P and Q intersects the curve at the point -R. The mirroring at the x-axis is the point R.
R is the result of the addition of P and Q.
P= (0.05/-1.45)
Q= (1.36/-2.69)
R = (-0.51/0.92)
R
-R
P
Q
y2 = x3 + 2.00x + 2.00
a = 2.00
b = 2.00
Zoom:
2 * P
P + Q
Delete points
Logfile
Quit