.۱

.۱.۱

$$\alpha^x = 3^{10} \ mod\ 31 = 25$$

$$(17,5):\ r = 17, s = 5 \quad \Rightarrow \quad t = \beta^r r^s \ mod\ p = \ 6^{17}17^5 \ mod\ 31 = 25 \quad \Rightarrow \quad valid$$

$$(13,5):\ r = 13, s = 5 \quad \Rightarrow \quad t = \beta^r r^s \ mod\ p = \ 6^{13}13^5 \ mod\ 31 = 5 \quad \Rightarrow \quad invalid$$

.۲.۱

تعداد امضاء های معتبر برای یک پیام x بستگی به مقدار k_E دارد و با توجه به این‌که k_E باید در محدوده 0 تا $p-2$ باشد، و همچنین شرط $\gcd(k_E, p-1) = 1$ باید برقرار باشد، بنابراین حداکثر برابر با $\Phi(p-1) = \Phi(30) = 8$ امضای معتبر داریم.

.۲

مهاجم از معادلات زیر استفاده کرده و برای x_1 ، x_2 ، s_1 و s_2 شناخته شده ابتدا کلید موقت k_E و سپس کلید خصوصی d را بدست می‌آورد.

$$s_1 \equiv (SHA(x_1) + dr)k_E^{-1} \ mod\ q$$

$$s_2 \equiv (SHA(x_2) + dr)k_E^{-1} \ mod\ q$$

$$s_1 - s_2 \equiv k_E^{-1}\big(SHA(x_1) - SHA(x_2)\big) \ mod\ q$$

$$\Rightarrow \ k_E = \frac{SHA(x_1) - SHA(x_2)}{s_1 - s_2} \ \ mod\ q$$

$$\Rightarrow d = \frac{s_1 \cdot k_E - SHA(x_1)}{r} \ \ mod\ q$$

.۳

$$s^{131} \equiv ?\, x \ mod\ 9797$$

$$x = 123, s = 6292 \ : \ 6292^{131} = 123 \equiv 123 \ mod\ 9797 \quad \Rightarrow \quad valid$$

$$x = 4333, s = 4768 \ : \ 4768^{131} = 9644 \neq 4333 \ mod\ 9797 \quad \Rightarrow \quad invalid$$

$$x = 4333, s = 1424 \ : \ 1424^{131} = 4333 \equiv 4333 \ mod\ 9797 \quad \Rightarrow \quad valid$$

۴.

$$t \approx \sqrt{2^{n+1} \cdot \ln\left(\frac{1}{1-\varepsilon}\right)}$$

۴	۴.۱	۴.۲
$length$	$\varepsilon = 0.5$	$\varepsilon = 0.1$
$64\ bit$	$\approx \sqrt{2^{64+1} \cdot \ln\left(\frac{1}{1-0.5}\right)}$ $= 2^{32}\sqrt{2 \cdot \ln(2)}$ $= 2^{32} \times 1.18$	$\approx \sqrt{2^{64+1} \cdot \ln\left(\frac{1}{1-0.1}\right)}$ $= 2^{32}\sqrt{2 \cdot \ln(10/9)}$ $= 2^{32} \times 0.46$
$128\ bit$	$\approx \sqrt{2^{128+1} \cdot \ln\left(\frac{1}{1-0.5}\right)}$ $= 2^{64}\sqrt{2 \cdot \ln(2)}$ $= 2^{64} \times 1.18$	$\approx \sqrt{2^{128+1} \cdot \ln\left(\frac{1}{1-0.1}\right)}$ $= 2^{64}\sqrt{2 \cdot \ln(10/9)}$ $= 2^{64} \times 0.46$
$160\ bit$	$\approx \sqrt{2^{160+1} \cdot \ln\left(\frac{1}{1-0.5}\right)}$ $= 2^{80}\sqrt{2 \cdot \ln(2)}$ $= 2^{80} \times 1.18$	$\approx \sqrt{2^{160+1} \cdot \ln\left(\frac{1}{1-0.1}\right)}$ $= 2^{80}\sqrt{2 \cdot \ln(10/9)}$ $= 2^{80} \times 0.46$

۵.

۱.۵

$$P(at\ least\ one\ Collision) = 1 - P(no\ Collision) =$$

$$1 - \prod_{i=1}^{n}\left(1 - \frac{i-1}{365}\right) \geq \frac{1}{2} \Rightarrow \prod_{i=1}^{n}\left(1 - \frac{i-1}{365}\right) \leq \frac{1}{2} \Rightarrow n = 23$$

$$\Rightarrow \prod_{i=1}^{23}\left(1 - \frac{i-1}{365}\right) = 0.49 \leq \frac{1}{2} \quad \Rightarrow n \geq 23$$

بنابراین باید حداقل ۲۳ نفر در یک کلاس وجود داشته باشند، تا حداقل دو دانش‌آموز با احتمال بیش‌تر از 0.5 تاریخ تولد یکسانی داشته باشند.

۲.۵.

$$P(at\ least\ one\ Collision) = 1 - P(no\ Collision)$$

$$= 1 - \prod_{i=1}^{K}\left(1 - \frac{i-1}{N}\right) = 1 - \prod_{i=0}^{K-1}\left(1 - \frac{i}{N}\right)$$

$$\xrightarrow{1-x \approx e^{-x}} 1 - \prod_{i=1}^{K-1} e^{-\frac{i}{N}} = 1 - e^{-\frac{1+2+\cdots+(K-1)}{N}} = 1 - e^{-\frac{K(K-1)}{2N}}$$

۶.

$$P(no\ Collision) = \left(1 - \frac{1}{2^n}\right)\left(1 - \frac{2}{2^n}\right)\cdots\left(1 - \frac{t-1}{2^n}\right) = \prod_{i=1}^{t-1}\left(1 - \frac{i}{2^n}\right)$$

$$\xrightarrow{1-x \approx e^{-x}} P(no\ Collision) = \prod_{i=1}^{t-1} e^{-\frac{i}{2^n}} = e^{-\frac{1+2+\cdots+(t-1)}{2^n}} = e^{-\frac{t(t-1)}{2\cdot 2^n}} = e^{-\frac{t(t-1)}{2^{n+1}}}$$

$$P(at\ least\ one\ Collision) = 1 - P(no\ Collision) = 1 - e^{-\frac{t(t-1)}{2^{n+1}}} = \varepsilon$$

$$\Rightarrow\ -\frac{t(t-1)}{2^{n+1}} = \ln(\varepsilon) \quad \Rightarrow \quad t(t-1) = 2^{n+1}\cdot\ln\left(\frac{1}{\varepsilon}\right)$$

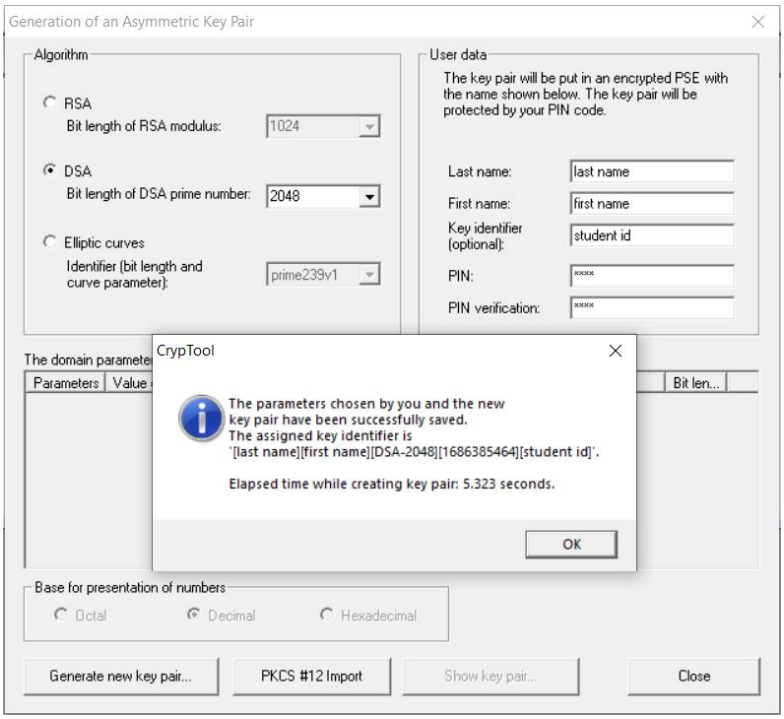
$$\Rightarrow\ t \approx \sqrt{2^{n+1}\cdot\ln\left(\frac{1}{1-\varepsilon}\right)}\ \approx\ 2^{(n+1)/2}\cdot\sqrt{\ln\left(\frac{1}{1-\varepsilon}\right)}$$

اگر $\varepsilon = 0.5$ باشد، آنگاه داریم:

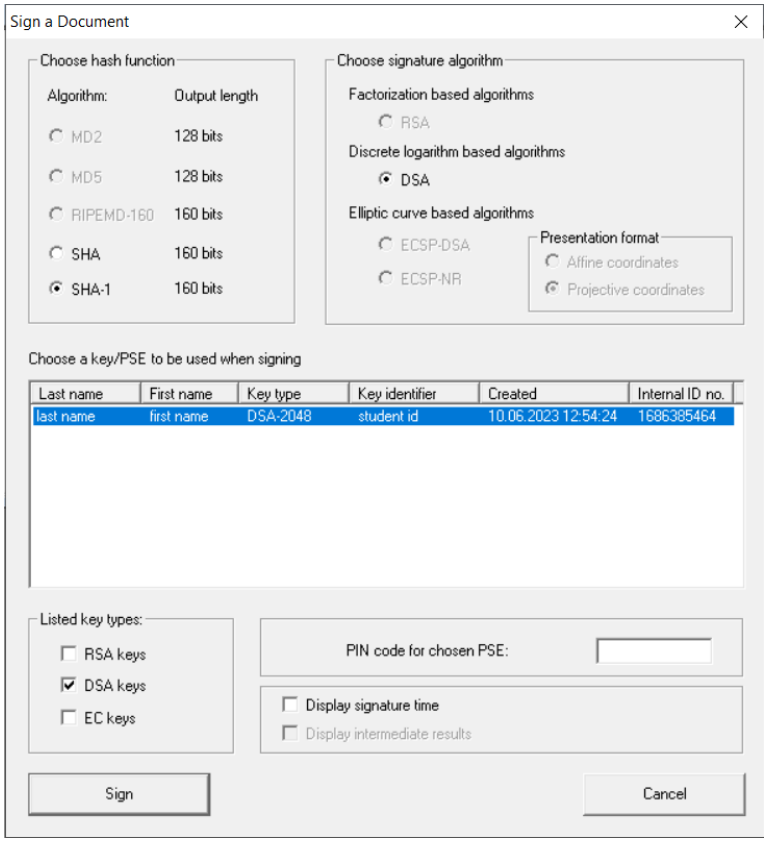
$$t \approx\ 2^{(n+1)/2}\cdot\sqrt{\ln\left(\frac{1}{1-0.5}\right)} =\ 2^{(n+1)/2}\cdot\sqrt{\ln(2)} =\ 2^{(n+1)/2}\cdot 0.833$$

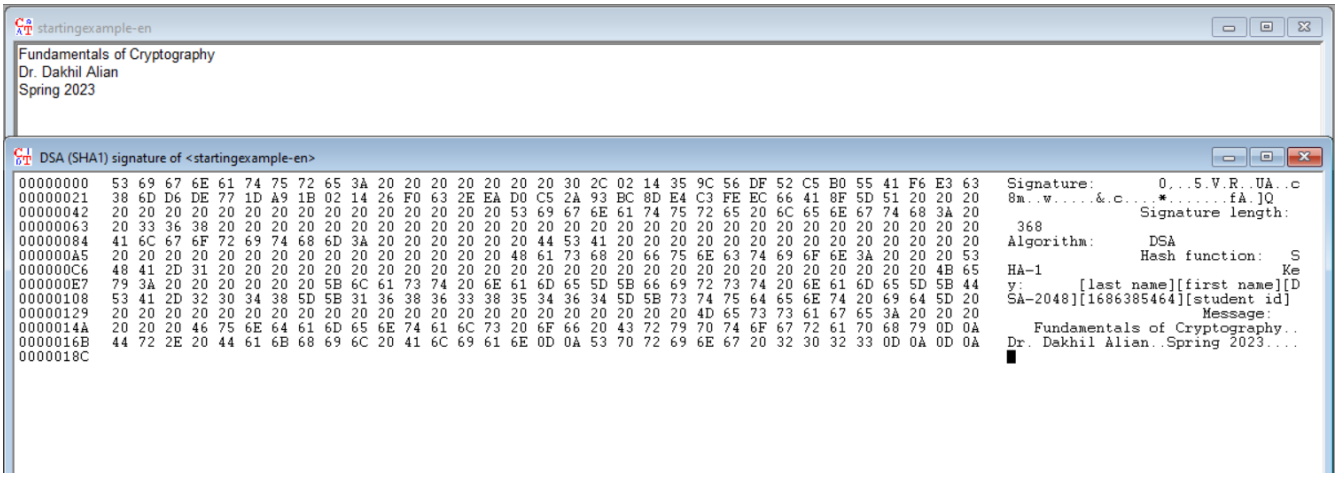
7.

a.


Generation of an Asymmetric Key Pair
Algorithm
RSA
Bit length of RSA modulus:
1024
DSA
Bit length of DSA prime number:
2048
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:
CrypTool
The parameters chosen by you and the new key pair have been successfully saved.
The assigned key identifier is '[last name][first name][DSA-2048][1686385464][student id]'.
Elapsed time while creating key pair: 5.323 seconds.
OK
Parameters
Value
Bit len...
Base for presentation of numbers
Octal
Decimal
Hexadecimal
Generate new key pair...
PKCS #12 Import
Show key pair...
Close

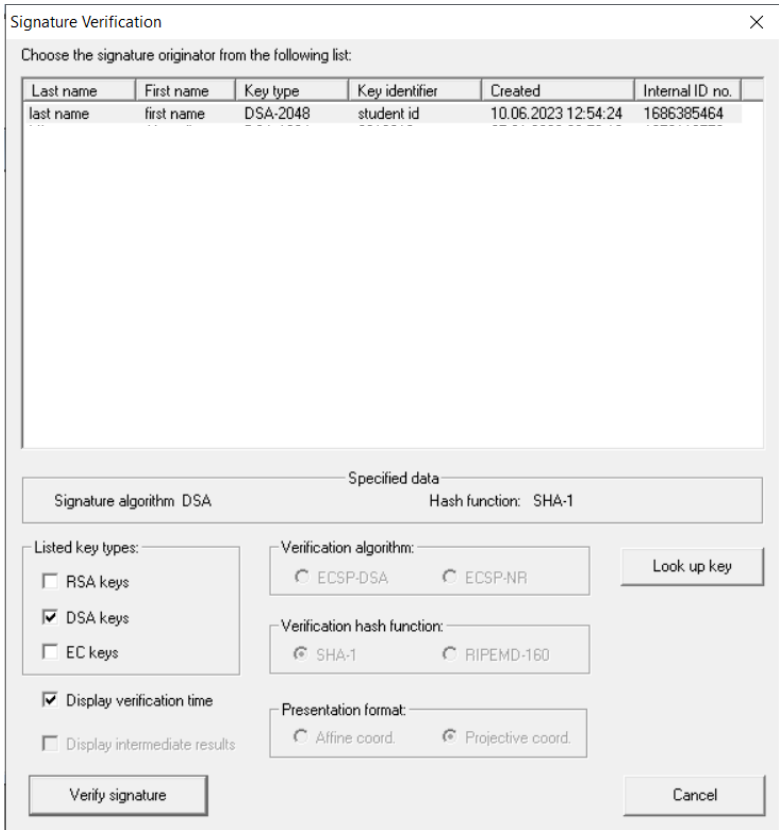
b.


Sign a Document
Choose hash function
Algorithm:
Output length
MD2
128 bits
MD5
128 bits
RIPEMD-160
160 bits
SHA
160 bits
SHA-1
160 bits
Choose signature algorithm
Factorization based algorithms
RSA
Discrete logarithm based algorithms
DSA
Elliptic curve based algorithms
ECSP-DSA
ECSP-NR
Presentation format
Affine coordinates
Projective coordinates
Choose a key/PSE to be used when signing
Last name
First name
Key type
Key identifier
Created
Internal ID no.
last name
first name
DSA-2048
student id
10.06.2023 12:54:24
1686385464
Listed key types:
RSA keys
DSA keys
EC keys
PIN code for chosen PSE:
Display signature time
Display intermediate results
Sign
Cancel

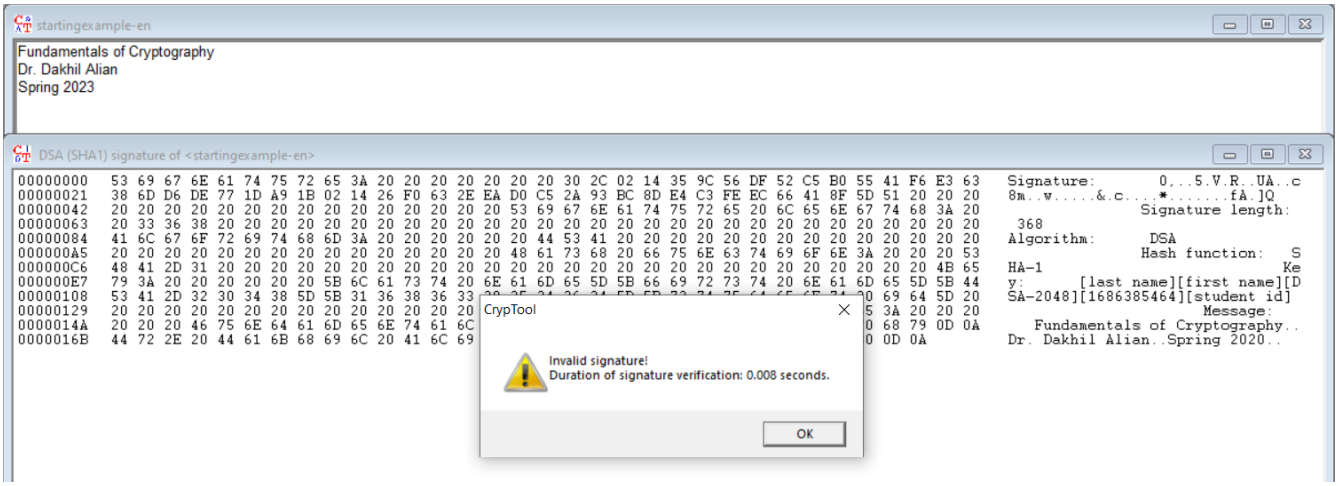


The file consists of the original document attached to its signature, which is signed using the DSA key.

c.



d.



Signatures will be computed using one's private key. Consequently, they can be decrypted using the same person's public key. As the public key is available to every other party, but the private key is unique to any individuals, only that specific person, who has the private key, can sign his own document. By signing files, we want to guarantee their integrity. Thus, if a document doesn't match the decrypted version of its attached signature, we assume it's been modified.