Exercises
Public-key cryptography

Carl Bootland – Bart Preneel

KU Leuven COSIC – Belgium
firstname.lastname@esat.kuleuven.be
http://www.esat.kuleuven.ac.be/∼preneel

November 2020

Public key cryptography – general – 1

Compute $9^9 \bmod 133$ using repeated squaring.

Extra: Compute $9^3 \bmod 133$. What can you deduce about $\lambda(133)$ without factoring 133? (Recall that for a positive integer n we have $a^{\lambda(n)} \equiv 1 \mod n$ for all a coprime to n.)

Public key cryptography – general – 1a

Write 9 in binary representation as 1001.
Then compute the required powers $9^{2^i} \mod 133$:

i	2^i	$9^{2^i} \mod 133$	
0	1	9	○
1	2	81	
2	4	44	
3	8	74	○

Multiplying the necessary terms from the table we reach:

$$9^9 \equiv 9 \cdot 74 \equiv 1 \mod 133.$$

Public key cryptography – general – 1b

Extra: We have that $9^3 \equiv 81 \cdot 9 \equiv 64 \bmod 133$.
Using the Euclidean algorithm there exists integers a and b such that $\gcd(9, \lambda(133)) = 9a + \lambda(133)b$.
Since we have that $9^9 \equiv 9^{\lambda(133)} \equiv 1 \mod 133$ we can deduce that also $9^{\gcd(9,\lambda(133))} \equiv 9^{9a+\lambda(133)b} \equiv (9^9)^a \cdot (9^{\lambda(133)})^b \equiv 1^a \cdot 1^b = 1 \mod 133$.
Now $9^3 \not\equiv 1 \mod 133$, thus $\gcd(9, \lambda(133) \neq 3$ and similarly $\neq 1$.
Hence we conclude $\gcd(9, \lambda(133)) = 9$ and thus $9 \mid \lambda(133)$.
Further $\lambda(133)$ must be even as $(-1)^r = -1$ for odd r (alternatively: $\lambda(n) = \mathrm{lcm}(p-1, q-1)$ hence it has to be even).

Hence $18 \mid \lambda(133)$ and in fact one can easily check by factoring 133 that $\lambda(133) = 18$.

Public key cryptography – general – 2

Compute efficiently $\varphi(100)$.

Public key cryptography – general – 2a

First we recall some properties of φ.
For a prime p and a positive integer a we have

$$\varphi(p^a) = p^a\left(1-\tfrac{1}{p}\right) = p^{a-1}(p-1).$$

Also for m and n coprime positive integers we have

$$\varphi(mn) = \varphi(m)\cdot\varphi(n).$$

Since we have $100 = 2^2\cdot 5^2$ we have

$$\varphi(100) = \varphi(2^2)\varphi(5^2) = 2^2\left(1-\tfrac{1}{2}\right)5^2\left(1-\tfrac{1}{5}\right) = 100\cdot\tfrac{1}{2}\cdot\tfrac{4}{5} = 40.$$

Public key cryptography – general – 3

Compute 10^{82} mod 33 without using repeated squaring.
Is 33 a strong pseudoprime to the base 10?

Public key cryptography – general – 3a

Euler's generalisation of Fermat's Little Theorem states that for a and n coprime we have

$$a^{\varphi(n)} \equiv 1 \mod n\,.$$

We have that $33 = 3\cdot 11$ so that $\varphi(33) = (3-1)(11-1) = 20$. Hence, as 10 and 33 are coprime, $10^{20} \equiv 1 \mod 33$ and therefore

$$10^{82} \bmod 33 = 10^{82 \bmod 20} \bmod 33 = 10^2 \bmod 33 = 1.$$

Since $33-1 = 2^5$ we have $v = 5,\ s' = 1$.
Also we have $10^{2^k} \equiv 1 \mod 33$ for $0 \le k < 5$.
As $10^{s'} = 10 \not\equiv 1 \mod 33$ and $10^{2^k\cdot s'} \equiv 1 \not\equiv -1 \mod 33$ for $0 \le k < 5$ we deduce that 33 is not a strong pseudoprime to the base 10, however it is a pseudoprime to the base 10.

Public key cryptography – general – 4

Compute gcd(1624, 6363).

Public key cryptography – general – 4b

Using the Euclidean Algorithm with inputs $a = 6363$ and $b = 1624$ we have

$$\begin{aligned} 6363 &= 3 \cdot 1624 + 1491 \\ 1624 &= 1 \cdot 1491 + 133 \\ 1491 &= 11 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0 \end{aligned}$$

and therefore we deduce that $\gcd(1624, 6363) = 7$ as 7 is the last non-zero remainder.

Public key cryptography – general – 5

Compute 101^{-1} mod 195.

Public key cryptography – general – 5a

Use the (Extended) Euclidean Algorithm. Recall at each step $i \geq 1$ we have the three equations

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i \qquad \text{where } 0 \leq r_{i+1} < |r_i| \\ s_{i+1} &= s_{i-1} - q_i s_i \\ t_{i+1} &= t_{i-1} - q_i t_i \end{aligned}$$

where initially $r_0 = 195$, $r_1 = 101$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$ and $t_1 = 1$. For each i we always have $r_i = 195 s_i + 101 t_i$.

i	r_i	q_i	s_i	t_i
0	195	–	1	0
1	101	1	0	1
2	94	1	1	-1

Public key cryptography – general – 5b

i	r_i	q_i	s_i	t_i
0	195	–	1	0
1	101	1	0	1
2	94	1	1	-1
3	7	13	-1	2
4	3	2	14	-27
5	1	3	-29	56

Therefore we have

$$1 = 195 \cdot (-29) + 101 \cdot 56,$$

thus $101 \cdot 56 \equiv 1 \bmod 195$ and so $101^{-1} \bmod 195 = 56$.

Public key cryptography – general – 6

Compute $5^{-1} \bmod 8$ using Euler's generalisation of Fermat's Theorem.

Extra:
What are the inverses of 3 and 7 modulo 8?
Deduce the value of $\lambda(8)$?
(In general, the Carmichael function of n, denoted $\lambda(n)$, is defined to be the minimal natural number λ such that $a^\lambda \equiv 1 \bmod n$ for all a coprime with n.)
If n is the product of two primes p and q, then $\lambda(n) = \operatorname{lcm}(p-1, q-1) = (p-1)\cdot(q-1)/\gcd(p-1, q-1)$.
If n is the product of three primes p, q and r, then $\lambda(n) = \operatorname{lcm}(p-1, q-1, r-1)$.

Public key cryptography – general –6a

We have $\varphi(8) = 8 \cdot \left(1 - \frac{1}{2}\right) = 4$. Therefore, using Euler's generalisation,

$5^{-1} \bmod 8 = 5^{4-1} \bmod 8 = 5^3 \bmod 8 = 25{\cdot}5 \bmod 8 = 1{\cdot}5 \bmod 8 = 5$.

Extra: Now $3^3 \bmod 8 = 27 \bmod 8 = 3$ and $7^3 \bmod 8 = (-1)^3 \bmod 8 = -1 \bmod 8 = 7$. Therefore each number between 0 and 8 that is coprime to 8 is its own inverse.
We deduce that $a^2 \equiv 1 \bmod 8$ for all a coprime to 8. Therefore $\lambda(8) = 2$.

Public key cryptography – general – 7

Find the smallest non-negative solution to the following system of congruences:

$$\begin{aligned} x &\equiv 4 \mod 19 \\ x &\equiv 7 \mod 11 \\ x &\equiv 1 \mod 7. \end{aligned}$$

Public key cryptography – general – 7a

Using the Chinese Remainder Theorem with $x_1 = 4$, $m_1 = 19$, $x_2 = 7$, $m_2 = 11$, $x_3 = 1$ and $m_3 = 7$ we compute

$$M_1 = 11 \cdot 7 = 77$$
$$M_2 = 19 \cdot 7 = 133$$
$$M_3 = 19 \cdot 11 = 209$$
$$M = 19 \cdot 11 \cdot 7 = 1463.$$

Also we compute

$$N_1 = 77^{-1} \bmod 19 = 1^{-1} \bmod 19 = 1$$
$$N_2 = 133^{-1} \bmod 11 = 1^{-1} \bmod 11 = 1$$
$$N_3 = 209^{-1} \bmod 7 = (-1)^{-1} \bmod 7 = -1 \bmod 7.$$

Then our required solution is

$$x = \sum_{i=1}^{3} x_i M_i N_i \bmod M = 4 \cdot 77 \cdot 1 + 7 \cdot 133 \cdot 1 + 1 \cdot 209 \cdot -1 \bmod 1463$$
$$= 308 + 931 - 209 \bmod 1463 = 1030 \bmod 1463 = 1030.$$

Public key cryptography – general – 8

What values can the order of a number mod 1001 take?
What is the order of 4 mod 1001?

Public key cryptography – general – 8a

The order of an integer a mod 1001 is the smallest positive power x such that $a^x \equiv 1$mod 1001.
First step is to factorise 1001.

- It is easy to find that the small prime that is a factor of 1001 is 7, hence $1001 = 7 \cdot 143$.
- We now check all prime numbers between 7 and $\sqrt{143} = 11.96$ and conclude that 11 divides 143.
  Thus $1001 = 7 \cdot 11 \cdot 13$.

Next we compute $\lambda(1001) = \text{lcm}(6, 10, 12) = \text{lcm}(2 \cdot 3, 2 \cdot 5, 2^2 \cdot 3) = 2^2 \cdot 3 \cdot 5 = 60$.
The order of a number mod 1001 is at most 60 and is a divisor of 60, that is, it belongs to the set $\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$.

Public key cryptography – general – 8a

The order of a number mod 1001 is at most 60 and is a divisor of 60, that is, it belongs to the set $\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$.
It is easy to see that $4, 4^2, 4^3, 4^4 < 1001$ hence the order of 4 is at least 5.
We know that $4^{60} \equiv 1 \bmod 1001$. We now take the prime divisors 2, 3 and 5 of 60 and verify that $4^{60/2} \equiv 1 \bmod 60$, $4^{60/3} \equiv 562 \bmod 60$ and $4^{60/5} \equiv 456 \bmod 60$.
Hence the order of 4 is a divisor of 30 but not of 20 and 12: the only options are 15 and 30. It is easy to verify that $4^{15} \equiv 155 \bmod 60$ hence the order of 4 is 30.

Note: once we have discovered that $4^{60/2} \equiv 1 \bmod 60$, we know that the order is a divisor of 30 and we can check immediately whether $4^{30/2} \equiv 1 \bmod 60$, $4^{30/3} \equiv 1 \bmod 60$, and $4^{30/5} \equiv 1 \bmod 60$.

Public key cryptography – general – 9

Determine all bases for which 15 is a pseudo-prime and for which 15 is a strong pseudo-prime.

definition:
Let s be an integer satisfying

$$a^{s-1} \equiv 1 \bmod s, \text{ for some } a,\ 1 < a < s$$

a *basis* a *pseudoprime* (notation: a-psp)

theorem (Fermat, 1640)
If s is prime and $\gcd(a, s) = 1$, then s is an a-psp

Public key cryptography – general – 9a

The integers $\{1, 2, 4, 7, 8, 11, 13, 14\}$ are relatively prime with 15.
$2^{14} \bmod 15 = 4$.
$4^{14} \bmod 15 = (2^{14})^2 \bmod 15 = 4^2 \bmod 15 = 1$.
$8^{14} \bmod 15 = (2^{14})^3 \bmod 15 = 4$.
$7^{14} \bmod 15 = 4$.
$11^{14} \bmod 15 = 1$.
$13^{14} \bmod 15 = 4$.
$14^{14} \bmod 15 = (-1)^{14} \bmod 15 = 1$.
Hence 15 is a pseudo-prime for the bases $\{4, 11, 14\}$.

Public key cryptography – 9b – Rabin-Miller

definition:
Let s be an odd integer with

$$s - 1 = 2^v \cdot s',\ \ s' \text{ odd.}$$

then s is a *strong basis* a *pseudoprime* (notation: strong basis a-psp) if either

$$a^{s'} \equiv 1 \bmod s$$

or

$$a^{2^k \cdot s'} \equiv -1 \bmod s, \text{for an integer } k,\ 0 \leq k < v$$

Public key cryptography – general – 9c

The Miller-Rabin test is more strict than the Fermat test, hence an integer s can only be a strong pseudo-prime for the basis a if it is a pseudo-prime for the basis a.
15 is a pseudo-prime for the bases $\{4, 11, 14\}$.

Decompose $15 - 1$ as $15 - 1 = 2^1 \cdot 7$.
Compute $4^7 \bmod 15 = 4$ while $4^{14} \bmod 15 = 1$.
Hence we have found that $4^7 \bmod 15 = 4$ and $(4^7)^2 \bmod 15 = 1$, or $4^7 \bmod 15 = 4$ is a square root of 1 different from $\{-1, 1\}$.

Compute $11^7 \bmod 15 = 11$, while $11^{14} \bmod 15 = 1$.
Hence 11 is a square root of 1 different from $\{-1, 1\}$.

Compute $14^7 \bmod 15 = (-1)^7 \bmod 15 = -1$.
This means that the Rabin-Miller condition is met for $k = 0$.

Hence 15 is a strong pseudo-prime for the bases $\{14\}$.

RSA – general – 1

Consider an RSA encryption-system with modulus $n = 629 = 37 \cdot 17$.
Choose the smallest possible public exponent.
What is the corresponding secret exponent?

RSA – general – 1a

We have $\varphi(629) = (37-1)\cdot(17-1) = 36 \cdot 16 = 576$ and $\gcd(36,16) = 4$.
Therefore $\lambda(629) = \mathrm{lcm}(37-1, 17-1) = (36)\cdot(16)/\gcd(36,16) = 576/4 = 144 = 2^4 3^2$.
We deduce that 5 is the smallest possible public exponent as it is the smallest positive integer coprime to $\lambda(n)$.
The secret exponent is then $5^{-1} \bmod 144$ and running the (Extended) Euclidean Algorithm we have the table

i	r_i	q_i	s_i	t_i
0	144	–	1	0
1	5	28	0	1
2	4	1	1	-28
3	1	4	-1	29

from which we can conclude that $5^{-1} \bmod 144 = 29$ is our secret exponent.

RSA – general – 2

Calculate the ciphertext for the message ‘591’.
Is there a problem?

RSA – general – 2a

The ciphertext is $c = m^e \bmod n = 591^5 \bmod 629$.
Using repeated squaring with the following table

i	2^i	$591^{2^i} \bmod 629$	
0	1	591	○
1	2	186	
2	4	1	○

we can compute that $591^5 \equiv 591 \cdot 1 \equiv 591 \bmod 629$ and so $c = 591$ and the ciphertext is the same as the message.
This is not a problem as to an eavesdropper this still looks like a random integer modulo 629.

RSA – general – 3

Decrypt your result using the Chinese Remainder Theorem; verify whether you retrieve the plaintext.

RSA – general – 3a

First we compute $x_1 = 591^{29} \bmod 37 = (-1)^{29} \bmod 37 = -1 \bmod 37$, and $x_2 = 591^{29} \bmod 17 = (-4)^{29} \bmod 17 = (-4)^{13} \bmod 17$. Now starting to use repeated squaring we find that $(-4)^2 = 16 \equiv -1 \mod 17$ so that $(-4)^4 \equiv 1 \bmod 17$.
Hence $(-4)^{13} \equiv (-4)^1 \bmod 17 = 13$ as $13 \bmod 4 = 1$.
We must therefore solve the congruences

$$\begin{aligned} x &\equiv -1 \mod 37 \\ x &\equiv -4 \mod 17 \end{aligned} \tag{1}$$

to find the plaintext.

RSA – general – 3b

Using the Chinese Remainder Theorem with $m_1 = 37 = M_2$ and $m_2 = 17 = M_1$ we compute

$$\begin{aligned} N_1 &= 17^{-1} \mod 37 = 24 \\ N_2 &= 37^{-1} \mod 17 = 3^{-1} \mod 17 = 6. \end{aligned}$$

and hence the message is

$$\begin{aligned} x &= -1 \cdot 17 \cdot 24 + -4 \cdot 37 \cdot 6 \mod 629 = -408 - 888 \mod 629 \\ &= -1296 \bmod 629 = 591. \end{aligned}$$

We have therefore verified that we have retrieved the correct plaintext.

Note: We could also have solved the two congruences $x \equiv 36$ mod 37 and $x \equiv 13 \bmod 17$ to arrive at the same result as these equations are equivalent to the equations above.

RSA – general – 4

Is it a problem to have a common modulus for RSA?
That is, suppose a message m is encrypted with both of the public keys (n, e) and (n, f), with $\gcd(e, f) = 1$, then can you break RSA given these two ciphertexts $c_e = m^e \mod n$ and $c_f = m^f \mod n$. If so, how?
(Hint: The Extended Euclidean Algorithm allows one to find integers x and y such that $\gcd(a, b) = xa + yb$.)

RSA – general – 4a

Run the Extended Euclidean Algorithm to find integers x and y such that $1 = \gcd(e, f) = ex + fy$. Then compute

$c_e^x \cdot c_f^y \mod n = (m^e)^x \cdot (m^f)^y \mod n = m^{ex+fy} \mod n = m \mod n.$

RSA – general – 5

Is a small public exponent e a security problem? Why?
(Hint: Suppose an entity wishes to send the same message m to three entities whose public moduli are n_1, n_2, n_3, and whose encryption exponents are all $e = 3$.)

RSA – general – 5a

Let the three messages be

$$c_1 = m^3 \mod n_1$$
$$c_2 = m^3 \mod n_2$$
$$c_3 = m^3 \mod n_3.$$

Then we have that m is the solution to the set of congruences:

$$m^3 \equiv c_1 \mod n_1$$
$$m^3 \equiv c_2 \mod n_2$$
$$m^3 \equiv c_3 \mod n_3.$$

If an eavesdropper captures the three ciphertexts c_1, c_2 and c_3 they can use the Chinese Remainder Theorem to compute the value of $m^3 \bmod n_1 n_2 n_3$ provided that n_1, n_2 and n_3 are coprime. (If they are not coprime then they can factor a modulus and compute the decryption key from which they can decrypt and find m directly.) Since $m < n_1, n_2, n_3$ we have that $m^3 < n_1 n_2 n_3$ and therefore that $m^3 \bmod n_1 n_2 n_3 = m^3$ over the integers. They can then take the cube root over the integers to compute m.

RSA – general – 6

Prove that if $n = pq$ is a product of two primes, then determining $\varphi(n)$ is equivalent to factoring n.

RSA − general − 6a

First, if we can factor n as the product of p and q then we can determine $\varphi(n)$ by computing $\varphi(n) = (p-1)(q-1)$.

Second, if we can determine $\varphi(n)$ then we claim that p and q are the roots of the following quadratic equation:

$$x^2 - (n+1-\varphi(n))x + n.$$

This is because we have

$$\begin{aligned}(x-p)(x-q) &= x^2 - (p+q)x + pq = x^2 - (pq - (p-1)(q-1) + 1)x + pq \\ &= x^2 - (n+1-\varphi(n))x + n.\end{aligned}$$

We can therefore compute the factors p and q of n using the quadratic formula:

$$p, q = \frac{n+1-\varphi(n) \pm \sqrt{(n+1-\varphi(n))^2 - 4n}}{2}.$$

RSA − general − 7

Suppose you have somehow gained access to the decryption device of a competitor who is using the basic RSA encryption scheme. You notice that their decryption times are extremely fast and you suspect their decryption exponent d is very small. You know that their public key is $(e, n) = (31, 247)$ and have intercepted the ciphertext $c = 23$.
Decrypt c without factoring n.

RSA − general − 7a

We suspect that d is very small and it must be odd so we can try the first few odd numbers greater than 1 as potential candidates for d. To test a candidate for d we can take a random message m and compute $m^{ed} \bmod n$. If this equals m then with good probability we have found the correct d. Testing more values of m we can become more confident in our guess for d.

We first try $d = 3$ and pick $m = 61$ (for example). Computing $61^{31\cdot 3} \bmod 247 = 235$ we deduce that $d \neq 3$.
Next we test $d = 5$, say with $m = 150$ and compute $150^{31\cdot 5} \bmod 247 = 80$; this shows that $d \neq 5$.
For $d = 7$ we choose randomly $m = 209$ and compute $209^{31\cdot 7} \bmod 247 = 209$ which suggest that $d = 7$. We can test more values of m and we find that $m^{31\cdot 7} \bmod 247 = m$ for all of them. We are now confident that $d = 7$.

RSA − general − 7b

Finally we can compute $c^7 \equiv 23^7 \equiv 101 \bmod 247$ as the decryption of c.

Aside: To be sure that we have the correct value of d we can attempt to factor n by using that $ed \equiv 1 \mod \lambda(n)$ and that $\lambda(n)$ is a divisor of $\varphi(n)$. Writing $ed = 1 + k\lambda(n)$ for some k and then $\varphi(n) = \ell\lambda(n)$ for some ℓ we can test small values of k and ℓ and use question 2 to attempt to compute p and q using our guess for $\varphi(n) = \ell(ed-1)/k$. In this case choosing $k = \ell = 1$ gives us p and q.

RSA – general – 8

You are told that the ACME RSA software builds an RSA modulus by choosing a random k-bit prime p and setting q to be the smallest prime larger than p. You manage to get hold of an RSA public key $(e, n) = (1921, 141367)$ and a ciphertext $c = 70918$ of someone using the ACME software. Decrypt the ciphertext.

RSA – general – 8a

Since p and q are consecutive primes they are the two closest primes to $\sqrt{n}$ with one being smaller and one being larger than $\sqrt{n}$. Computing $\sqrt{141367} = 375.988\ldots$ we look for the first prime q after 375. It does not take long to find that $q = 379$ is this prime and we compute $p = n/q = 373$ as the other factor of n.

Now we can compute $\varphi(n) = 372 \cdot 378 = 140616$ and $\lambda(n) = 140616/6 = 23436$. Then $d = e^{-1} \bmod 23436 = 61$. Finally we can decrypt the ciphertext $c = 70918$ by computing $70918^{61} \bmod 141367 = 100001$.

ElGamal – 1

Given $p = 89$, $a = 3$, $y = 69$. Verify for a message $m = 77$ whether the signature $(r, s) = (66, 77)$ is a valid signature.

ElGamal – 1a

Given $p = 89$, $a = 3$, $y = 69$. Verify for a message $m = 77$ whether the signature $(r, s) = (66, 77)$ is a valid signature.

We have

$a^m = 3^{77} \bmod 89 = 77$ and $y^r \cdot r^s = 69^{66} \cdot 66^{77} = 88 \cdot 12 \bmod 89 = 77$.

Therefore since

$$a^m \equiv y^r \cdot r^s \bmod p$$

the signature is valid.

ElGamal – 2

Show that a different random number k must be selected for each message signed; otherwise the private key x can be determined with high probability.

ElGamal – 2a

Suppose that the signer signs two messages m_1 and m_2 with the same random value k and let the signatures be respectively:

$$(r_1, s_1) = \left(a^k \mod p, (m_1 - xr_1)k^{-1} \mod (p-1)\right)$$
$$(r_2, s_2) = \left(a^k \mod p, (m_2 - xr_2)k^{-1} \mod (p-1)\right).$$

Thus we see that $r_1 = r_2 = r$ and we have the two congruences involving xr:

$$s_1 = (m_1 - xr)k^{-1} \mod (p-1)$$
$$s_2 = (m_2 - xr)k^{-1} \mod (p-1)$$

or equivalently

$$xr \equiv m_1 - s_1 k \equiv m_2 - s_2 k \mod (p-1).$$

ElGamal – 2b

Rearranging gives the congruence

$$(s_2 - s_1)k \equiv m_2 - m_1 \mod (p-1)$$

and if $(s_2 - s_1)$ is invertible modulo $p-1$ then we can solve for k. If $\gcd(s_2 - s_1, p-1) = d$ then there are d solutions for k and for each of them we can compute $a^k \bmod p$ and only for the correct value of k will the result be r. Once we know k we can try to solve the congruence

$$xr \equiv m_1 - s_1 k \mod (p-1).$$

If r is invertible modulo $p-1$ there is a unique solution for x. Otherwise if $\gcd(r, p-1) = d'$ then there are d' solutions and we can determine the correct value for x by checking whether $a^x \equiv y \mod p$ for each possible solution.