Public-key Cryptography

Exercise Session

Mariana Gama
mariana.botelhodagama@kuleuven.be

November 2023

Some remarks - 1

Euler's totient function

$\varphi(n)$ denotes the number of positive integers less than n which are relatively prime to n

- For p prime, $\varphi(n) = p - 1$.
- For p^k with p prime, $\varphi(p^k) = p^k \left(1 - \frac{1}{p}\right)$

To understand the expression for $\varphi(p^k)$, note that there is a total of p^k integers from 1 to p^k and then count how many of them are **not** relatively prime to p^k.

The integers not relatively prime to p^k will be the multiples of p, and there are p^{k-1} such multiples which are less than p^k. Therefore,

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k \left(1 - \frac{1}{p}\right)$$

Some remarks - 1

Euler's totient function

Because the Euler function is multiplicative, we get that for $n = \prod_i p_i^{k_i}$

$$\varphi(n) = \prod_i p_i^{k_i}\left(1 - \frac{1}{p_i}\right)$$

Note that the multiplicativity of the Euler function follows from the Chinese Remainder Theorem only holds for integers that are coprime. That is, if $\gcd(a, b) \neq 1$ then $\varphi(ab) \neq \varphi(a) \cdot \varphi(b)$.

Some remarks - 2

Charmichael function

- For p prime, $\lambda(p) = p - 1$.
- For p and q prime, $\lambda(p \cdot q) = \text{lcm}[p-1, q-1]$.
- For $n = p_1^{k_1} \ldots p_m^{k_m}$, $\lambda(n) = \text{lcm}\left[\lambda(p_1^{k_1}), \ldots, \lambda(p_m^{k_m})\right]$, where

$$\lambda(p_i^{k_i}) = \begin{cases} 2^{k_i - 2} & \text{if } p_i = 2 \text{ and } k_i > 2, \\ p_i^{k_i - 1}(p_i - 1) & \text{otherwise.} \end{cases}$$

Just like for Euler's totient function, we have that for a and n coprime,

$$a^{\lambda(n)} \equiv 1 \mod n$$

However, $\lambda(n)$ is the **smallest** positive integer for which the previous congruence holds for every integer a between 1 and n that is coprime with n. This means that $\lambda(n)$ divides $\varphi(n)$.

Some remarks - 3

Chinese Remainder Theorem (proof with r congruences)

We want to find x such that

$$\begin{aligned} x &\equiv x_1 \mod m_1 \\ x &\equiv x_2 \mod m_2 \\ &\dots \\ x &\equiv x_r \mod m_r \end{aligned}$$

where $\gcd(m_i, m_j) = 1$.

Let $m = m_i \dots m_r$. We want to find α_i such that $x \equiv \sum_i \alpha_i \cdot x_i \mod m$. In order for x to be a solution, we need that:

$$\alpha_i \equiv 1 \mod m_i \quad (1)$$

$$\alpha_i \equiv 0 \mod m_j, \text{for } j \neq i \quad (2)$$

It follows from (2) that $\alpha_i = \alpha_i' \cdot \prod_{j \neq i} m_j = \alpha_i' \cdot (m/m_i)$.

Some remarks - 3

Chinese Remainder Theorem (proof with r congruences)

We now find α'_i using (1):

$$\alpha'_i \cdot (m/m_i) \equiv 1 \mod m_i$$

Note that $\gcd(m/m_i, m_i) = 1$, so

$$\alpha'_i \equiv (m/m_i)^{-1} \mod m_i$$

The expression for each α_i is thus:

$$\alpha_i \equiv (m/m_i) \cdot \left[(m/m_i)^{-1} \mod m_i\right] \mod m$$

and

$$x \equiv \sum_i x_i \cdot (m/m_i) \cdot \left[(m/m_i)^{-1} \mod m_i\right] \mod m$$

Public-key cryptography - 1

Compute $5^{-1} \mod 11$.

Euler's Theorem
For a and n coprime,

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

This means that $a^{\varphi(n)-1}$ is an inverse of $a \mod n$.

We know that for p prime, $\varphi(p) = p - 1$, so $\varphi(11) = 10$.
Therefore,

$$5^{-1} \mod 11 \equiv 5^9 \mod 11.$$

We can now compute $5^9 \mod 11$ using repeated squaring.

Public-key cryptography - 1

We can now compute $5^9 \mod n$ using repeated squaring.

Write 9 in binary representation as 1001.

i	2^i	$5^{2^i} \mod 11$
0	1	5
1	2	3
2	4	9
3	8	4

From the binary representation, we know we will need the terms corresponding to $i = 0$ and $i = 3$. Multiplying the necessary terms:

$$5^9 \equiv 5 \cdot 4 \equiv 9 \mod 11$$

(Verify that $5 \cdot 9 \equiv 1 \mod 11$.)

Public-key cryptography - 2

Compute $101^{-1} \mod 195$.

We now use the **Extended Euclidean Algorithm**
Recall that if we run it with inputs a and b, we get

$$at + bs = \gcd(a, b).$$

Since $\gcd(101, 195) = 1$, we will get x and y such that $101t + 195s = 1$. Hence, $t = 101^{-1} \mod 195$.

Public-key cryptography - 2

For each step $i \geq 1$ of the algorithm we have three equations:

$$r_{i+1} = r_{i-1} - q_i r_i$$

$$s_{i+1} = s_{i-1} - q_i s_i$$

$$t_{i+1} = t_{i-1} - q_i t_i$$

with $r_0 = 195$, $r_1 = 101$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$.
For each i, $r_i = 195 s_i + 101 t_i$.

Public-key cryptography - 2

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,

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

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

Public-key cryptography - 2

Instead of building the previous table, we can also do the (regular) Euclidean Algorithm and them do back substitution.

$$\begin{aligned} 195 &= 1 \cdot 101 + 94 \\ 101 &= 1 \cdot 94 + 7 \\ 94 &= 13 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

The non-zero last remainder corresponds to the $\gcd(195, 101)$, which we knew was 1 since the numbers are coprime.

Public-key cryptography - 2

Now we can back substitute:

$$\begin{aligned}
1 &= 7 - 2 \cdot 3 \\
&= 7 - 2 \cdot (94 - 13 \cdot 7) = 27 \cdot 7 - 2 \cdot 94 \\
&= 27 \cdot (101 - 1 \cdot 94) - 2 \cdot 94 = 27 \cdot 101 - 29 \cdot 94 \\
&= 27 \cdot 101 - 29 \cdot (195 - 1 \cdot 101) = 56 \cdot 101 - 29 \cdot 94
\end{aligned}$$

Again, we obtained $1 = 56 \cdot 101 - 29 \cdot 94$.

Public-key cryptography - 3

Three users have RSA moduli $n_1 = 87$, $n_2 = 115$ and $n_3 = 187$ respectively. They use exponent $e = 3$. We see the following ciphertexts on the communication channel: $c_1 = 5$, $c_2 = 20$ and $c_3 = 181$. We suspect that these ciphertexts correspond to a unique message. Find this message.

We know three moduli and the ciphertexts. If these ciphertexts correspond to the same message, then we know that:

$$
\begin{aligned}
5 &\equiv m^3 \quad \mod 87 \\
20 &\equiv m^3 \quad \mod 115 \\
181 &\equiv m^3 \quad \mod 187
\end{aligned}
$$

Public-key cryptography - 3

So we know that m^3 is the solution to the set of congruences:

$$m^3 \equiv 5 \mod 87$$
$$m^3 \equiv 20 \mod 115$$
$$m^3 \equiv 181 \mod 187$$

Notice that $87 = 3 \cdot 29$, $115 = 5 \cdot 23$ and $187 = 11 \cdot 17$, so these three numbers are coprime.
We can then use the Chinese Remainder Theorem to compute

$$m^3 \mod 87 \cdot 115 \cdot 187$$

Public-key cryptography - 3

Let $n_1 = 87$, $n_2 = 115$, $n_3 = 187$. Then,

$$M = n_1 \cdot n_2 \cdot n_3 = 1870935$$
$$M_1 = n_2 \cdot n_3 = 115 \cdot 187 = 21505$$
$$M_2 = n_1 \cdot n_3 = 87 \cdot 187 = 16269$$
$$M_3 = n_1 \cdot n_2 = 87 \cdot 115 = 10005$$
$$N_1 = M_1^{-1} \mod n_1 = 21505^{-1} \mod 87 = 16^{-1} \mod 87 = 49$$
$$N_2 = M_2^{-1} \mod n_2 = 16269^{-1} \mod 115 = 54^{-1} \mod 115 = 49$$
$$N_3 = M_3^{-1} \mod n_3 = 10005^{-1} \mod 187 = 94^{-1} \mod 187 = 2$$

$$m^3 = c_1 \cdot M_1 \cdot N_1 + c_2 \cdot M_2 \cdot N_2 + c_3 \cdot M_3 \cdot N_3 \mod M$$

Substituting the values we get $m^3 = 512000 \mod M$.

Public-key cryptography - 3

Since $m < n_1, n_2, n_3$ we have that $m^3 < n_1 n_2 n_3$ and therefore $m^3 \mod n_1 n_2 n_3 = m^3$ over the integers.

We can now calculate $m = 512000^{1/3} = 80$.

Public-key cryptography - 4

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.

An ElGamal signature has the form (r, s) where

$$r \equiv a^k \mod p$$
$$s \equiv (M - x \cdot r) \cdot k^{-1} \mod (p - 1)$$

- p is a large prime number
- a is a generator in $[2, p - 1]$
- M is a message in $[0, p - 1]$
- Choose secret key x in $[2, p - 1]$
- Set the public key $y \equiv a^x \mod p$.

For each message, choose k in $[0, p - 1]$ with $\gcd(k, p - 1)$ at random. Set $r \equiv a^k \mod p$

Public-key cryptography - 4

If two messages M_1 and M_2 are encrypted with the same k, we get

$$\begin{aligned} r_1 &= r_2 = r \\ s_1 &\equiv (M_1 - x \cdot r) \cdot k^{-1} \mod (p-1) \\ s_2 &\equiv (M_2 - x \cdot r) \cdot k^{-1} \mod (p-1) \end{aligned}$$

Note now that $(s_1 - s_2)k \equiv (M_1 - M_2) \mod (p-1)$. If $\gcd(s_1 - s_2, p-1) = 1$, then $(s_1 - s_2)$ is invertible modulo $p-1$ and so

$$k \equiv (s_1 - s_2)^{-1}(M_1 - M_2) \mod (p-1).$$

Note that if $\gcd(s_1 - s_2, p-1) = d$, then there are d solutions for k. We can compute $a^k \mod p$ for each one of them and compare to the public value r in order to find the correct k.

Public-key cryptography - 4

If r is invertible modulo $p-1$, there is a single solution for x:

$$x \equiv (M_1 - k \cdot s_1) \cdot r^{-1} \mod (p-1)$$

Otherwise, if $\gcd(r, p-1) = d'$, there will be d' solutions for x. We can check the correct one by computing $a^x \mod p$ and comparing to the public key y for each one of them.

Public-key cryptography - 4

To see why $\gcd(a, m) = d$ implies there are that there are d solutions to $ax \equiv b \mod m$, note that this congruence means that $ax - b$ is a multiple of m. Since d divides both a and m, then it must also divide b.

We can now rewrite $a = a'd$, $b = b'd$ and $m = m'd$. Then we get that $a'dx \equiv b'd \mod m'd$. Since $m'd$ divides $a'dx - b'd$, we must also have that m' divides $a'x - b$, and so $a' \equiv b' \mod m'$.

Because d was the greatest common divisor of a and m, a' and m' must be relatively prime. Therefore, a' is invertible $\mod m'$ and thus $a' \equiv b' \mod m'$ has a unique solution $x \equiv (a')^{-1}b' \mod m'$.

To find the solutions to the original congruence, we need to find the integers $\mod m$ which are congruent to $x \mod m'$. These are the numbers of the form $x + im'$, where i ranges from 0 to $d - 1$.