MA080G Cryptography Assignment Block 1

Viktor Rosvall

May 14, 2019

Question 2

a. Explain the operation of the RSA public-key cryptosystem.

b. Illustrate your explanation by using the primes $p = 13$ and $q = 17$ and secret decryption key $d = 103$ to

   (i) decrypt the ciphertext $z = 2$;

   (ii) compute the public encryption key e corresponding to d;

   (iii) encrypt the plaintext $m = 2$

c. Discuss the security of the RSA public-key cryptosystem.

Answer 2

a. RSA works by generating a public and private key-pairs from very large primes. The public key can be only be used to decrypted data encrypted using the private key, and vice versa.

Encryption is done in Z_n, where n is the product of two primes, p and q.

RSA Encryption: given the public key $(n, e) = k_{pup}$, and the plaintext x.

$$y = e_{k_{\text{pup}}}(x) \equiv x^e \pmod{n}$$

where $x, y \in Z_n$, and e is called the encryption exponent or public exponent.

Decryption is similarly done in Z_n.

RSA Decryption: given the private key $d = k_{priv}$, and the plaintext x.

$$x = d_{k_{\text{priv}}}(y) \equiv y^d \pmod{n}$$

where $x, y \in Z_n$, and d is called the decryption exponent or private exponent.

Key Generation of a public key $(n, e) = k_{pup}$ and a private key $d = k_{priv}$. This means we have to calculate n, e and d.

RSA Key Generation
1. Compute $n = p * q$, where p and q are two large primes.
2. Compute $\Phi(n) = (p-1)(q-1)$
3. Choose a large **public exponent** $e \in \{1, 2, ..., \Phi(n)-1\}$ such that the

$$\gcd(e, \Phi(n)) = 1.$$

4. Compute the **private exponent** d such that

$$d * e \equiv 1 \pmod{\Phi(n)}$$

thus $d = e^{-1}$.

When calculating Euclid's algorithm for the gcd we can calculate the linear combination calculated from the Extended Euclid's Algorithm (EEA). This gives us both e and d.

b. (i) We are given that $p = 13$, $q = 17$ and $d = 103$. First we need to calculate what integer ring we are working in, i.e., $n = 13 * 17 = 221$.
We are given that the ciphertext $y = z = 2$, so to calculate x we use the formula $x = y^d \equiv \pmod{n}$
2^{103} is a pretty big number so we can't really use calculators on it, especially not on even bigger numbers. So we need to reduce d to something smaller. This can be achieve by using this rule:

$$ab \text{ MOD } n = ((a \text{ MOD } n)(b \text{ MOD } n)) \text{ MOD } n$$

So we begin by reducing 2^{103} MOD 221:

$$\begin{aligned} x = 2^{103} \text{ MOD } 221 &= ((2^{50} \text{ MOD } 221)(2^{53} \text{ MOD } 221)) \text{ MOD } 221 \\ &= ((2^{25} \text{ MOD } 221)(2^{25} \text{ MOD } 221)(2^{25} \text{ MOD } 221)(2^{28} \text{ MOD } 221)) \text{ MOD } 221 \\ &= (2 * 2 * 2 * 16) \text{ MOD } 221 \\ &= 2^7 \text{ MOD } 221 \\ &= 128 \end{aligned}$$

and $x = 128$ is the plaintext as $x = 2^{103} \equiv 2^7 \equiv 128 \equiv \pmod{221}$

(ii) Recall from the generation of keys, that e is chosen from the $\gcd(e, \Phi(n)) = 1$. The EEA of $(e, \Phi(n))$ also gave us d.
We know that d is the inverse of e since $d * e \equiv 1 \pmod{\Phi(n)}$. Thus we can calculate e by doing the EEA of $(d, \Phi(n))$ as they are inverses in Z_n.

First we begin by calculating the EEA of $(103, \Phi(221))$:

$$\begin{array}{llll} 192 & = 103 * 1 + 89 & 89 & = 192 - 103(1) \\ 103 & = 89 * 1 + 14 & 14 & = 103 - 89(1) \\ 89 & = 14 * 6 + 5 & 5 & = 89 - 14(6) \\ 14 & = 5 * 2 + 4 & 4 & = 14 - 5(2) \\ 5 & = 4 * 2 + 1 & 1 & = 5 - 41) \end{array}$$

Then we can calculate the linear equation $1 = s * \Phi(n) + t * d$, where t is the inverse of d.

$$\begin{aligned} 1 &= 5 - 4(1) \\ &= 5(3) - 14(1) \\ &= 89(3) - 14(19) \\ &= 89(22) - 103(19) \\ &= 192(22) - 103(41) \end{aligned}$$

Thus $d^{-1} = e = t = -41$. But $e \notin \{1, 2, ..., \Phi(n) - 1\}$. So we need to choose the class representative of e in $Z_{\Phi(n)}$, thus:

$$e = [-41] = [151], \text{ in } Z_{192}.$$

(iii) From (i) and (ii) we have calculated that $n = 221$ and $e = 151$. The formula for encrypting plaintext x into ciphertext y is:

$$y \equiv x^e \pmod{n}$$

The plaintext $x = m = 2$ encrypted is:

$$y = 2^{151} \pmod{221}$$

$2^{151} \pmod{221}$ can be calculated using **Modular Exponentiation**.

$$\begin{array}{llll} 2^1 & = 2^1 & \equiv 2^1 \text{ MOD } 221 & = 2 \\ 2^2 & = (2^1)^2 & \equiv 2^2 \text{ MOD } 221 & = 4 \\ 2^4 & = (2^2)^2 & \equiv 4^2 \text{ MOD } 221 & = 16 \\ 2^8 & = (2^4)^2 & \equiv 16^2 \text{ MOD } 221 & = 35 \\ 2^{16} & = (2^8)^2 & \equiv 35^2 \text{ MOD } 221 & = 120 \\ 2^{32} & = (2^{16})^2 & \equiv 120^2 \text{ MOD } 221 & = 35 \\ 2^{64} & = (2^{32})^2 & \equiv 35^2 \text{ MOD } 221 & = 120 \\ 2^{128} & = (2^{64})^2 & \equiv 120^2 \text{ MOD } 221 & = 35 \end{array}$$

Next we need to actually calculate $2^{151} \pmod{221}$, we need 151 in binary: $151_{10} = 1001011_2$.

$$\begin{aligned} 2^{151} \text{ MOD } 221 &= (2^{128}2^{16}2^4 2^2 2^1) \text{ MOD } 221 \\ &\equiv (35 * 120 * 16 * 4 * 2) \text{ MOD } 221 \\ &= 128 \end{aligned}$$

c. Since RSA is based on the multiplying two large primes to get the modulus n. If we are able factorize n, we could calculate $\Phi(n)$ which is required if we want to find inverse of the public key (as we did in b. (ii)).

Question 3

a. Let $p \geq 2$ be a prime. Define what it means for an integer a to be a primitive element modulo p.

b. Find a primitive element modulo 23 and prove that it is a primitive element.

Answer 3

a. The element a is called the *generator* or a *primitive element* of the group G, if $\text{ord}(a) = |G|$.

Recall from Fermat's Little Theorem that, when p is prime and a is any integer

$$a^{p-1} \equiv 1 \pmod{p}$$

also gives that a is a primitive element of mod p.

Powers of a primitive element a in mod p can be used to express every non-zero element in Z_p.

b. 5 is a primitve element in mod 23, since $5^{22} \equiv 1$ MOD 23.

Question 4

c. Let a and n be positive integers and let $n \geq 2$. Prove that if $\gcd(a, n) = 1$ then

$$a^{\Phi(n)} \equiv 1 \pmod{n}.$$

d. Discuss whether the theorem from part (c) can be used as a primality test.

Answer 4

c. Recall from **Euler's theorem** that if $\gcd(a, n) = 1$, then $a^{\Phi(n)} \equiv \pmod{n}$.

Proof: let $\{x_1, x_2, ..., x_m\} \in Z_n^*$, i.e., the integers x relative prime to n in Z, where $m = \Phi(n)$.

Suppose that the $\gcd(a, n) = 1$, then a has a multiplicative inverse b mod n. So

$$ab \equiv 1 \pmod{n}.$$

Let $y_i = ax_i \pmod{n}$, where $i = 1, 2, ..., m$.

The $\gcd(y_i, n) = 1$, since $\gcd(a, n) = \gcd(x_i, n) = 1$. And $y_1, ..., y_m$ is distinct, because $y_i \neq y_j$.

Thus the sets $y_1, ..., y_m$ and $x_1, ..., x_m$ is equal, so their products are also the same:

$$\prod x_i = \prod y_i \equiv \prod a x_i \pmod{n} = a^m \prod x_i \pmod{n}.$$

And since we know that x has an inverse since the $\gcd(x_i, n) = 1$, we can multiply the inverse product:

$$a^m \prod x_i * \prod x^{-1} \equiv \prod x_i * \prod x^{-1} \pmod{n}$$
$$a^m \equiv 1 \pmod{n}$$

d. No it cannot be used to determine if an integer is prime or not. Fermat's Little Theorem can be used to determine if an integer is prime or not in most cases. It will give false positives on Carmichael Numbers.

Question 6

For positive integers $p \geq 2$, Wilson's Theorem states that

$$p \text{ is a prime if and only if } (p-1)! \equiv -1 \pmod{p}.$$

a. Prove Wilson's Theorem.

b. Discuss whether Wilson's Theorem is suitable as a primality test for finding primes to use with RSA.

Answer 6

a. Assume p is prime. Then all the integer $a \in \{1, 2, ..., p-1\}$ are coprime to p. This means that each integer have an inverse b such that $ab \equiv -1 \pmod{p}$. This can be expressed as:

$$1 * 2 * ... * (p-1) \equiv -1 \pmod{p}$$

or as the theorem

$$(p-1)! \equiv -1 \pmod{p}$$

b. It's not suitible since when using RSA, want to have very large primes. Computing $p!$ on a very large prime is impossible, as it would take forever.