MAS433 Cryptography: Tutorial 4
Public Key Encryption and Digital Signature
19.11.2010

Problem 1. Toy RSA
In a toy RSA encryption scheme, $n = 209$, $e = 7$. Find the value of the private key d. Decrypt the ciphertext $c = 3$.

Problem 2. RSA: Common Modulus
Two users Alice and Bob use RSA public keys with the same modulus n but with different public exponents e_1 and e_2.

(a) Prove that Alice can decrypt messages sent to Bob.

(b) Suppose that message padding is not used in RSA encryption. Prove that Eve can decrypt a message sent to Alice and Bob provided that $\gcd(e_1, e_2) = 1$. (Hint: how to find a and b satisfying $a \times e_1 + b \times e_2 = 1$)

Problem 3. RSA: $\lambda(n)$
In RSA, d can be computed as $e \cdot d \equiv 1 (\mathrm{mod} \lambda(n))$, where

$$\lambda(n) = \frac{(p-1)(q-1)}{gcd(p-1, q-1)}.$$

(a) Prove that encryption and decryption are inverse operations.

(b) Let $n = 209$, $e = 7$. Find the value of the private key d. Decrypt the ciphertext $c = 3$.

Problem 4. RSA: small difference between p and q
The p and q in RSA should be randomly generated, and they are the same size. The difference between p and q should not be small.

(a) Suppose that p and q are 1024-bit prime numbers, but the difference between p and q is small, say, $u = |p - q| < 2^{32}$. How to factorize the product of p and q?

(b) Suppose that $u = |p - q| < 20$, and $p \times q = 2189284635403183$. Find the values of p and q.

Problem 5. Dixon's Random Squares Algorithm
Factorize 256961 using Dixon's Random Squares Algorithm. The factor base {-1,2,3,5,7,11,13,17,19,23,29,31} may be used.

Problem 6. Toy ElGamal Encryption
In a toy ElGamal encryption scheme, $p = 227$, $g = 2$, and $x = 15$. Decrypt the ciphertext (10, 159).

Problem 7. Index Calculus Algorithm
Let $p = 227$. The element $g = 2$ is a generator of the multiplicative group Z_p^*.

(a) Compute g^{32}, g^{40}, g^{59} and g^{156} modulo p, and factorize them.

(b) Find the values of $\log_g 2 \mod p$, $\log_g 3 \mod p$, $\log_g 5 \mod p$, $\log_g 7 \mod p$, and $\log_g 11 \mod p$.

(c) Suppose that we wish to compute $\log_g 173 \mod p$. Multiply 173 by $g^{177} \mod p$, and factorize the result. What is the value of $\log_g 173 \mod p$?

Problem 8. RSA Signature Scheme
Suppose that hash function is not used in RSA digital signature scheme. The signature is generated as $s = m^d \mod n$. Given a message m and its signature s, how to modify m without being detected?

Problem 9. ElGamal Signature Scheme

(a) In the Elgamal signature scheme, why should the signature with $s = 0$ be deleted?

(b) In the Elgamal signature scheme, each per-message secret integer k should be used only once. If the per-message secret integer k is reused, how to attack this digital signature algorithm?

(c) In the Elgamal signature scheme, each per-message secret integer k should be randomly generated. If the per-message secret integer k is generated as follows: k_0 is randomly generated, $k_{i+1} = k_i + a$, where a is a known constant. Develop an attack to recover the private key.

(d) In the ElGamal signature scheme, each per-message secret integer k should be randomly generated. If the per-message secret integer k is generated as follows: k_0 is randomly generated, $k_{i+1} = k_i + a$, where a

is a large unknown constant. Develop an attack to recover the private key .

Problem 10. Digital Signature Algorithm (DSA)

(a) In the Digital Signature Algorithm, if the per-message secret integer k is reused, how to attack this digital signature algorithm?

(b) In a modified DSA, s is generated as $s = k^{-1}(H(m) - xr) \mod q$. What is the signature verification algorithm for this modified DSA?

(c) Let p and q be prime numbers and q is a divisor of $p-1$. Show that for any integer t, if $g = h^{(p-1)/q} \mod p$, then $g^t \mod p = g^{t \mod q} \mod p$.

Problem 11. Unconditionally secure and computationally secure
Is there unconditionally secure public key cryptosystem? Briefly explain why.