Homework Assignment 4 - Introduction To Cryptography

Ton That Tam Dinh

October 22, 2017

Problem 3.6.

Proof. (a) Bob's ciphertext is: $c \equiv m^e \equiv 45293 (modN)$
(b) We have N = 2038667 = 1301 * 1567, so $\phi(n) = 1300 * 1566 = 2035800$
Base on $\phi(n)$ we have $d \equiv e^{-1} \equiv 810367 (mod\phi(n))$
(c) Bob's message is: $m \equiv c^d \equiv 514407 (modN)$

□

Problem 3.7.

Proof. By factoring N we have N = 73 * 167, so it can be easily to compute $\phi(n) = 72 * 166 = 11952$. In the next step, we will compute d by the formula: $d \equiv e^{-1} \equiv -323 \equiv 11629 (mod\phi(n))$. Finally, we have Allice's message: $m \equiv c^d \equiv 4894 (modN)$

□

Problem 3.9.

Proof. Because we have $a^{de} \equiv 1 (modn)$ so $de \equiv 1 (mod\phi(n))$

(a)

(b) We will try to find p, q such that: $d_1e_1 = 1 + k_1 * (pq - (p + q) + 1)$ and $d_2e_2 = 1 + k_2 * (pq - (p + q) + 1)$ (notice that pq = N). And found p + q = 12594. Then we have pq = N = 38749709, and p + q = 12594. Using Vieta Theorem, p,q is two solution of equation: $x^2 - (p + q)x + pq = 0$. Solving this equation, we have p = 5347, q = 7247.
(c) We have (d_1, e_1) = (70583995, 491157), (d_2, e_2) = (173111957, 7346999), (d_3, e_3) = (180311381, 29597249)

We will try to find p, q such that: $d_1e_1 = 1 + k_1 * (pq - (p + q) + 1)$, $d_2e_2 = 1 + k_2 * (pq - (p + q) + 1)$, and $d_3e_3 = 1 + k_3 * (pq - (p + q) + 1)$, with

(notice that pq = N). And found p + q = 31574. Then we have pq = N = 225022969, and p + q = 31574. Using Vieta Theorem, p,q is two solution of equation: $x^2 - (p+q)x + pq = 0$. Solving this equation, we have p = 10867, q = 20707.
(d) We have (d_1, e_1) = (1103927639, 76923209), (d_2, e_2) = (1022313977, 106791263), (d_3, e_3) = (387632407, 7764043)

We will try to find p, q such that: $d_1e_1 = 1 + k_1 * (pq - (p + q) + 1)$, $d_2e_2 = 1 + k_2 * (pq - (p + q) + 1)$, and $d_3e_3 = 1 + k_3 * (pq - (p + q) + 1)$, with

(notice that pq = N). And found p + q = 110442. Then we have pq = N = 1291233941, and p + q = 11042. Using Vieta Theorem, p,q is two solution of equation: $x^2 - (p+q)x + pq = 0$. Solving this equation, we have p = 13291, q = 97151.

□

Problem 3.10.

Proof. (a) We need prove x equal to m, it means m is solution of the pair of congruences (because CRT tell that there is one solution in modulo pq): $x \equiv c_1 (modp)$ and $x \equiv c_2 (modq)$ so we just need to prove $m \equiv mg^{r_1 * (p-1) * s_1} (modp)$ and $m \equiv mg^{r_2 * (q-1) * s_1} (modq)$. It means we need to prove $g^{r_1 * (p-1) * s_1} \equiv 1 (modp)$ and $g^{r_1 * (q-1) * s_1} \equiv 1 (modq)$.

We only have two congruences since (g, N) = 1. So i think it's the weakness of cryptosystem, and make it's not secure.

(b) This cryptosystem is not secure because we only have solution when random number g sastify (g, N) = 1.

□

Problem 3.12.

Proof. We have $gcd(e_1, e_2) = gcd(102763679, 519424709) = 1$ so it exist two integer u, v such that $e_1 * u + e_2 * v = 1$. By using extended Euclide algorithm, we find that u = 252426389 and v = -496549570.

We also have $c_1 \equiv m^{e_1} (modN)$ and $c_2 \equiv m^{e_2} (modN)$, then we can write $m^1 \equiv m^{e_1 * u + e_2 * v} \equiv (c_1)^u * (c_2)^v \equiv 1031756109 * 603385073 \equiv 1054592380 (modN)$

□