ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

Handout 20 Introduction to Communication Systems

Solutions to Homework 11 December 4, 2008

PROBLEM 1. 1. (a) Assume that d divides b. Since $d = \gcd(a, m)$, from the Bezout's identity we have,

$$d = \alpha a + \beta m$$

for some integers α, β. Since d divides b we have $b = dk$ for some integer k. Thus $d = \frac{b}{k}$. Thus

$$\frac{b}{k} = \alpha a + \beta m$$
$$b = (k\alpha)a + k\beta m$$

which implies that m divides $a(k\alpha) - b$. Thus we can set $x = k\alpha$ as the solution of the congruence equation.

(b) Since the congruence equation has a solution, there exists an integer x such that

$$ax - b = mq \tag{1}$$

for some integer q. Dividing by d we get

$$\frac{a}{d}x - \frac{b}{d} = \frac{m}{d}q$$

since d is the $\gcd(a, m)$, d divides both a, m. As a result we have

$$\frac{b}{d} = \frac{a}{d}x - \frac{m}{d}q$$

The r.h.s of the above equation is an integer, which implies that d divides b.

2. We have

$$ac - bc = mq$$

for some integer q. Dividing by $d = \gcd(c, m)$ we get

$$a\frac{c}{d} - b\frac{c}{d} = \frac{m}{d}q$$

Now since d is the $\gcd(c, m)$, we have that $\gcd(\frac{c}{d}, \frac{m}{d}) = 1$, thus from the above equation we must have that $\frac{m}{d}$ divides $a - b$, which proves the statement.

PROBLEM 2. From the problem we can formulate the following two congruence equations for k:

$$2k \equiv 4 \pmod 5$$
$$5k \equiv 30 \pmod{35}$$

To solve this we can use the Chinese remainder theorem. We can covert the above congruences to the standard form by using part 2 of the previous problem. Thus we have

$$\begin{aligned} k &\equiv 2 \pmod 5 \\ k &\equiv 6 \pmod 7 \end{aligned}$$

using $c = 2, m = 5$ for the first congruence and $c = 5, m = 35$ for the second congruence. We can now solve the above by extended Euclid. The answer is any $x \equiv 27 \pmod{35}$.

Problem 3. In this problem we notice that in order to compute a^b we can look at the binary representation of $b = b_0 + 2b_1 + 2^2b_2 + 2^3b_3 + \cdots + 2^kb_k$ where $b_i \in \{0, 1\}$ and thus compute the numbers $a, a^2, a^4, a^8, \ldots, a^{2^k}$, where 2^k is the nearest power of 2 less than or equal to b. To compute these numbers we require at the most $\log_2 b$ operations. Indeed, given a we get a^2 in one operation. From a^2 we get $a^4 = (a^2)(a^2)$ in one operation. With a^4 we get $a^8 = (a^4)(a^4)$ in one operation and so on we get a^{2^k} in at most $\log_2 b$ operations. Now to compute a^b, we compute $a^{b_k 2^k} \cdot a^{b_{k-1}2^k} \cdots a^{b_0}$ which requires at the most $\log_2 b$ operations. Thus total operations required is at most $2\log_2 b$.

Problem 4.

1. We need to find k which is the inverse of K modulo $\phi(131 \times 137)$. Here $k = 3969$.

2. The number corresponding to the plaintext $\alpha\beta\gamma$ is given by $26^2N_\alpha + 26N_\beta + \gamma$, where N_α is the number of the letter α etc. This is clear since we are ordering each triplet of letters lexicographically. Thus the group THE maps to the number $26^2 \times 19 + 26 \times 7 + 4 = 13030$.

3. We use the normal RSA scheme to get the plaintext *GRADED*.

Problem 5. The digital signature is just the standard RSA with the roles of k, K reversed. But all the calculations to show that RSA works can be replicated for this case in a straightforward manner. Indeed Asquare can verify by the public key K as follows:

$$\begin{aligned} D_K(C) \pmod m &= D_K(E_k(P)) \pmod m \\ &= (P^k)^K \pmod m = (P^K)^k \pmod m \\ &= D_k(E_K(P)) \pmod m \\ &= P \end{aligned}$$

the last equation is true because K, k are public, private keys of the RSA scheme.

Their love is safe with very high probability because Babubhai may try various attacks. (i) Trying to find a key k_1 such that $Kk_1 \equiv 1 \pmod{\phi(m)}$ is very difficult, since it involves the knowledge $\phi(m)$ which is very difficult to determine if $m = pq$ with p, q being very large prime numbers. (ii) He may try to solve $C \equiv P^k \pmod m$ to find Yakari's private key k. He is then faced with the *discrete logarithm* problem which is again very difficult to solve if m is very large. (iii) If he changes the poem P to P_1 then Asquare can decrypt and realise that $D_K(C) \neq P_1$.