Cryptography I, homework sheet 4
Due: 08 October 2010, 10:45

1. Find the smallest positive integer x satisfying the following system of congruences, should such a solution exist.
$$\begin{aligned} x &\equiv 0 \bmod 3 \\ x &\equiv 1 \bmod 5 \\ x &\equiv 2 \bmod 8 \end{aligned}$$

2. Find the smallest positive integer x satisfying the following system of congruences, should such a solution exist.
$$\begin{aligned} x &\equiv 3 \bmod 4 \\ x &\equiv 6 \bmod 12 \end{aligned}$$

3. Find the smallest positive integer x satisfying the following system of congruences, should such a solution exist.
$$\begin{aligned} x &\equiv 4 \bmod 9 \\ x &\equiv 10 \bmod 12 \end{aligned}$$

4. Users A, B, C, D, and E are friends of S. They have public keys $(e_A, n_A) = (5, 62857), (e_B, n_B) = (5, 64541), (e_C, n_C) = (5, 69799), (e_D, n_D) = (5, 89179)$, and $(e_E, n_E) = (5, 82583)$. You know that S sends the same message to all of them and you observe the ciphertexts $c_A = 11529, c_B = 60248, c_C = 27504, c_D = 43997$, and $c_E = 44926$. What was the message?

Theorem 1 (Chinese Remainder Theorem)
Let $r_1, \dots, r_k \in \mathbb{Z}$ and let $0 \neq n_1, \cdots, n_k \in \mathbb{N}$ such that the n_i are pairwise coprime. The system of equivalences
$$\begin{aligned} X &\equiv r_1 \bmod n_1, \\ X &\equiv r_2 \bmod n_2, \\ &\vdots \\ X &\equiv r_k \bmod n_k, \end{aligned}$$
has a solution X which is unique up to multiples of $N = n_1 \cdot n_2 \cdots n_k$. The set of all solutions is given by $\{X + aN | a \in \mathbb{Z}\} = X + N\mathbb{Z}$.

If the n_i are not all coprime the system might not have a solution at all. E.g. the system $X \equiv 1 \bmod 8$ and $X \equiv 2 \bmod 6$ does not have a solution since the first congruence implies that X is odd while the second one implies that X is even. If the system has a solution then it is unique only modulo $\mathrm{lcm}(n_1, n_2, \dots, n_k)$. E.g. the system $X \equiv 4 \bmod 8$ and $X \equiv 2 \bmod 6$ has solutions and the solutions are unique modulo 24. Replace $X \equiv 2 \bmod 6$ by $X \equiv 2 \bmod 3$; the system still carries the same information and we obtain $X = 8a + 4 \equiv 2a + 1 \overset{!}{\equiv} 2 \bmod 3$, thus $a \equiv 2 \bmod 3$ and $X = 8(3b + 2) + 4 = 24b + 20$. The smallest positive solution is thus 20.

We now present a constructive algorithm to find this solution, making heavy use of the extended Euclidean algorithm presented in the previous section. Since all n_i are coprime, we have $\gcd(n_i, N/n_i) = 1$ and we can compute u_i and v_i with

$$u_i n_i + v_i(N/n_i) = 1.$$

Let $e_i = v_i(N/n_i)$, then this equation becomes $u_i n_i + e_i = 1$ or $e_i \equiv 1 \bmod n_i$. Furthermore, since all $n_j | (N/n_i)$ for $j \neq i$ we also have $e_i = v_i(N/n_i) \equiv 0 \bmod n_j$ for $j \neq i$.
Using these values e_i a solution to the system of equivalences is given by

$$X = \sum_{i=1}^{k} r_i e_i,$$

since X satisfies $X \equiv r_i \bmod n_i$ for each $1 \leq i \leq k$.

Example 2 *Consider the system of integer equivalences*

$$\begin{aligned} X &\equiv 1 \bmod 3, \\ X &\equiv 2 \bmod 5, \\ X &\equiv 5 \bmod 7. \end{aligned}$$

The moduli are coprime and we have $N = 105$. For $n_1 = 3, N_1 = 35$ we get $v_1 = 2$ by just observing that $2 \cdot 35 = 70 \equiv 1 \bmod 3$. So $e_1 = 70$. Next we compute $N_2 = 21$ and see $v_2 = 1$ since $21 \equiv 1 \bmod 5$. This gives $e_2 = 21$. Finally, $N_3 = 15$ and $v_3 = 1$ so that $e_3 = 15$.
The result is $X = 70 + 2 \cdot 21 + 5 \cdot 15 = 187$ which indeed satisfies all 3 congruences. To obtain the smallest positive result we reduce 187 modulo N to obtain 82.

For easier reference we phrase this approach as an algorithm.

Algorithm 3 (Chinese remainder computation)
IN: *system of k equivalences as $(r_1, n_1), (r_2, n_2), \ldots (r_k, n_k)$ with pairwise coprime n_i*
OUT: *smallest positive solution to system*

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. $X \leftarrow 0$
3. `for` $i = 1$ `to` k
   (a) $M \leftarrow N \operatorname{div} n_i$
   (b) $v \leftarrow ((N_i)^{-1} \bmod n_i)$ *(use XGCD)*
   (c) $e \leftarrow vM$
   (d) $X \leftarrow X + r_i e$
4. $X \leftarrow X \bmod N$