T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 5: Solutions
11.–12.3.2003

1. Let $g\colon \{0,1\}^n \to \{0,1\}^n$ be a one-way function, and define $h\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$ by $h(x,y) = (g(x) \oplus y, y)$. Suppose h is not one-way, and $z \in \{0,1\}^n$ is given. Then we can find x,y such that $h(x,y) = (z,0)$. But since $h(x,y) = (g(x) \oplus y, y) = (z,0)$, we must have $y = 0$ and $g(x) = z$. This contradicts the one-wayness of g. It follows that h is a one-way function.

   If we apply the construction in the exercise to this particular h, we get $h^*(x,y) = ((g(x) \oplus y) \oplus x, y \oplus y) = (g(x) \oplus y \oplus x, 0)$. If $(z,0)$ is given, $h^*(z, g(z)) = (g(z) \oplus g(z) \oplus z, 0) = (z,0)$. Thus h^* is not one-way.

   For this particular one-way function, the construction fails.

2. Suppose h is not one-way. Let A be an inverter for h (that is, $A(y)$ produces a value x such that $h(x) = y$). We will construct an algorithm B that finds collisions in h with probability at least 0.5. By repeating the algorithm, we can find a collision with arbitrarily high probability. The algorithm B works as follows:

   - Pick a random $x \in \{0,1\}^n$ and compute $y = h(x)$.
   - Compute $x' = A(x)$.
   - If $x \neq x'$, return (x,x') (collision found), otherwise return $\perp$ (failure).

   The computation performed by B is dominated by the computation of A. It remains to compute the success probability of B.

   Define $x \sim x' \iff h(x) = h(x')$. This is clearly an equivalence relation. Let
   $$[x] = \{x' \mid x \sim x'\}$$
   denote the equivalence class of x, and denote $(x) = |[x]|$. Let furthermore $\mathcal{C}$ denote the set of all equivalence classes.

   Since each equivalence class $[x]$ is the inverse image of some $y \in \{0,1\}^m$, there can be at most 2^m equivalence classes. Let x be the element chosen in the first step of the algorithm. For this x, there are (x) elements that could be returned in the second step. Of these, $(x) - 1$ are different from x and leads to success of B. Since x is randomly chosen, and A is only given $y = h(x)$, The probability that $A(x) \in [x] - \{x\}$ is $((x) - 1)/(x)$. Thus, the success probability for this x is
   $$\frac{(x) - 1}{(x)} \ .$$
   The total success probability is
   $$\begin{aligned}\Pr[\text{success}] &= 2^{-n} \sum_{x \in \{0,1\}^n} \frac{(x)-1}{(x)} = 2^{-n} \sum_{c \in \mathcal{C}} \sum_{x \in C} \frac{|c|-1}{|c|} = 2^{-n} \sum_{c \in \mathcal{C}} (|c| - 1) \\ &= 2^{-n} \Big(\sum_{c \in \mathcal{C}} |c| - |\mathcal{C}| \Big) = \frac{2^n - |\mathcal{C}|}{2^n} \geq \frac{2^n - 2^m}{2^n} \geq \frac{2^n - 2^{n-1}}{2^n} = \frac{1}{2} \ .\end{aligned}$$

3. Computing $5^{12345678}$ directly would yield a 8629259-decimal number and is therefore inpractical. We instead use the following well-known "square and multiply"-algorithm. To compute $a^b \bmod n$, do:

   - Initialise $x = 1$ and $y = a$ (x will hold the result while y will hold consecutive squares of a).
   - While $b > 0$, do
     - If b is odd, set $x \leftarrow x \cdot y \bmod n$.
     - Set $b \leftarrow \lfloor b/2 \rfloor$.
     - Set $y \leftarrow y \cdot y \bmod n$.
   - Return x.

   Using this algorithm, we can compute

$$5^{12345678} \bmod 100000007 = 35073282 \ .$$

4. (a) The Euclidean algorithm gives:

$$\begin{aligned} 274 &= 54 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1. \end{aligned}$$

   Eliminating the remainders one by one, we get

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 \\ &= 5 - 1 \cdot (274 - 54 \cdot 5) = 55 \cdot 5 - 1 \cdot 274. \end{aligned}$$

   Thus, $55 \cdot 5 = 1 + 1 \cdot 274$, or $55 \cdot 5 \equiv 1 \pmod{274}$. That is, $5^{-1} \equiv 55 \pmod{274}$.

   (b) Proceeding as above, we get:

$$\begin{aligned} 1155 &= 4 \cdot 278 + 43 \\ 278 &= 6 \cdot 43 + 20 \\ 43 &= 2 \cdot 20 + 3 \\ 20 &= 6 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

   Moving backwards, we get:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (20 - 6 \cdot 3) = 7 \cdot 3 - 1 \cdot 20 \\ &= 7 \cdot (43 - 2 \cdot 20) - 1 \cdot 20 = 7 \cdot 43 - 15 \cdot 20 \\ &= 7 \cdot 43 - 15 \cdot (278 - 6 \cdot 43) = 97 \cdot 43 - 15 \cdot 278 \\ &= 97 \cdot (1155 - 4 \cdot 278) - 15 \cdot 278 = 97 \cdot 1155 - 403 \cdot 278. \end{aligned}$$

   Thus, $278^{-1} \equiv -403 \equiv 752 \pmod{1155}$.

5. Since $\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$ and $q = n/p$, we have $n - p - n/p + 1 = \phi(n)$, or $p^2 - (n - \phi(n) + 1)p + n = 0$. This is an ordinary quadratic equation for p. Its solutions

$$\frac{n - \phi(n) + 1}{2} \pm \sqrt{\frac{(n - \phi(n) + 1)^2}{4} - n}$$

give the factors p and q of n.