TMA4155 — Solutions to exercise 4

Kristian Gjøsteen

2005-09-21

Task 1 — MACs

a. We know that $f(k,x) = t$. This means that we know one thing about the function $\tilde{f}(k,\cdot)$, namely that $\tilde{f}(k,x) = t_0$.

Note that for a message $x||y$ consisting of two blocks x and y, the CBC-MAC $f(k,x||y) = \tilde{f}(k,\tilde{f}(k,x) \oplus y)$. If we can force the input to the outer evaluation to be x, then we know that the resulting output will be t_0. So if we set $y = x \oplus t_0$, we get that

$$f(k,x||y) = \tilde{f}(k,\tilde{f}(k,x) \oplus y) = \tilde{f}(k,t_0 \oplus (x \oplus t_0)) = \tilde{f}(k,x) = t_0.$$

b. Let $m' \in \{0,1\}^n$ be arbitrary. Then

$$t' = f(k,m||m') = h(k||m||m') = h'(h'(h'(0,k),m),m').$$

If we know $t = f(k,m) = h'(h'(0,k),m)$, we can compute

$$t' = h'(t,m').$$

Task 2 — RSA cryptosystem

a. We are given $p = 5$, $q = 7$ and $e = 5$. Then $n = pq = 35$, and d should be an inverse to $e = 5$ modulo $(p-1)(q-1) = 4 \cdot 6 = 24$. It is easy to see that $5 \cdot 5 \equiv 25 \equiv 1 \pmod{24}$, so $d = 5$ is ok.

This gives the public key $pk = (35,5)$ and the secret key (private key) $sk = (35,5)$.

b. $6^5 \equiv 6^{2^2} \cdot 6 \equiv 36^2 \cdot 6 \equiv 1^2 \cdot 6 \equiv 6 \pmod{35}$.

c. $17^5 \equiv 17^{2^2} \cdot 17 \equiv 9^2 \cdot 17 \equiv 11 \cdot 17 \equiv 12 \pmod{35}$.

Task 3 — Greates common divisor

a. $\gcd(153, 157) = 1$.

b. $\gcd(153, 187) = 17$.

c. $\gcd(10005, 1101) = 3$.

d. $\gcd(10005, 1103) = 1$.