Solutions to Problem Set 6

Problem 23: ElGamal Signatures

If $k = a$, then $\beta = r$, so Eve can notice this from Alice's public key (p, α, β) and any signed message triple (m, r, s) at once. In order to get k, Eve only needs to solve $s \equiv k^{-1}(m - ar) \equiv k^{-1}m - r \pmod{p-1}$. Rewrite the above equation to $(s + r)k \equiv m \pmod{p-1}$. If $\gcd(s + r, p-1) > 1$, then Eve will get $\gcd(s+r, p-1)$ solutions, but she can still check $r \equiv \alpha^k \pmod{p}$ to find out the correct value.

Problem 24: Hash Functions

(a) Let $H(x) = h_1(x) \cdot h_2(x)$, in which $\cdot$ means concatenation. We will show that $H(x)$ is definitely strongly collision-free, otherwise, assume one can find a colliding pair (m, m') for H. Then $h_1(m) \cdot h_2(m) = h_1(m') \cdot h_2(m')$. And then we have $h_1(m) = h_1(m')$ and $h_2(m) = h_2(m')$, which contradicts that one of h_1 and h_2 is strongly collision-free.

(b) If $E_k(b) = k \otimes b$, then

$$\begin{aligned}
f_1(s, b) &= E_s(b) \otimes b = s \otimes b \otimes b = s \\
f_2(s, b) &= E_s(b) \otimes b \otimes s = s \otimes b \otimes b \otimes s = 0 \\
f_3(s, b) &= E_s(b \otimes s) \otimes b = s \otimes b \otimes s \otimes b = 0 \\
f_4(s, b) &= E_s(b \otimes s) \otimes b \otimes s = s \otimes b \otimes s \otimes b \otimes s = s
\end{aligned}$$

So for H_1 and H_4, the output results are always equal to IV, while for H_2 and H_3, the results are always 0. Therefore, none of these hash functions is strongly collision-free.

Problem 25: Simplified Feige-Fiat-Shamir Authentication Protocol

If Irma knows the sequence of b, he can break the system easily by generating many valid pairs (x, y). For $b = 0$, he can generate a valid pair (x, y) by choosing $y \in Z_n$ and $x \equiv y^2 \pmod{n}$. For $b = 1$, he can just let $y \in Z_n$ and $x \equiv y^2 v \pmod{n}$. So if Happy uses such a trivial sequence of b, Irma will soon discover the pattern and make correct guesses for any successive b.

Problem 26: Secret Sharing Basics

(a) We can just use Shamir secret sharing scheme to solve this problem. Let $p = 7$, and choose $s_0 = 5, s_1 = 2$, then we have the polynomial $s(x) \equiv 5 + 2x \pmod{p}$ and give each person a pair (x_i, y_i) with $y_i \equiv s(x_i) \pmod{p}$. For example, $(1, 0), (2, 2), (3, 4), (4, 6)$. Then any two persons can just solve the linear system to obtain s_0.

(b) We know $i = 20$ and $M + si = 97$, so we obtain $M + 20s = 97$ in which both M and s are positive integers. So the possible values for s are $\{1, 2, 3, 4\}$ and for M are $\{77, 57, 37, 17\}$ respectively.

Problem 27: Secret Sharing with Cheater

The foreign agent can be found as long as his pair doesn't satisfy the polynomial $s(x)$. We can randomly pick any two persons and solve the linear system to get $s'(x)$, e.g. we pick A and B. And then we check the remaining two persons' pairs with $s'(x)$, i.e. C and D's pairs. If there is exactly one pair which doesn't satisfy $s'(x)$, we know $s'(x)$ is correct and the person holding the wrong pair is the foreign agent. If neither pair satisfies $s'(x)$, then we know the foreign agent is among the two persons we just choose, e.g. A or B. We then recompute $s(x)$ with C and D's pairs and check A and B with this correct polynomial.

So when we try to solve the linear system with A and B's pairs, we get $s'(x) = 8 + 7x$. And then we check C and D and find only C doesn't satisfy $s'(x)$, so C is the foreign agent and the message is 8.