Homework Set 10

Problem 1

Example 25. Consider the following compression function $C(x)$ which takes three bits input and outputs two bits:

x	000	001	010	011	100	101	110	111
$C(x)$	10	00	11	01	01	10	00	11

Let $H(x)$ be the hash function obtained from $C(x)$ using the Merkle–Damgård construction (using initial value $h_1 = 0$). Compute $H(11000)$.

Solution. Here, $b = 2$ and $c = 1$, so that each x_i is 1 bit: $x_1x_2x_3x_4x_5 = 11000$.

$h_1 = 00$

$h_2 = C(h_1, x_1) = C(001) = 00$

$h_3 = C(h_2, x_2) = C(001) = 00$

$h_4 = C(h_3, x_3) = C(000) = 10$

$h_5 = C(h_4, x_4) = C(100) = 01$

$h_6 = C(h_5, x_5) = C(010) = 11$

Hence, $H(11000) = h_6 = 11$.

Problem 2

Example 26. Bob's public RSA key is $(N, e) = (35, 19)$. His private key is $d = 19$. For signing, Bob uses the (silly) hash function $H(x) = x \pmod{22}$. Determine Bob's signature s of the message $m = 361$.

Solution. $H(m) = 361 \pmod{22} = 9$. The signature therefore is $s = H(m)^d \pmod{N} = 9^{19} \equiv 9 \pmod{35}$.

Problem 3

Example 27. Alice uses an RSA signature scheme and the (silly) hash function $H(x) = x_1 + x_2$, where $x_1 = 3x \pmod{11}$ and $x_2 = 2x \pmod{29}$, to sign the message $m = 1299$ with the signature $s = 121$. Forge a second signed message.

Solution. Since we have no other information, in order to forge a signed message, we need to find another message with the same hash value as $m = 1299$. From our experience with the Chinese remainder theorem, we realize that changing x by $11 \cdot 29$ does not change $H(x)$. Since $1299 + 11 \cdot 29 = 1618$, a second signed message is $(1618, 121)$.

Armin Straub
straub@southalabama.edu