

MATH 470 Homework 8

[1] Let $n = pq$ where p, q are distinct large primes and let x be the set of messages converted to numbers in the range $(10\sqrt{n}, \infty)$ (using padding if necessary). Let h be the hash function $h(x) = x^2 \pmod{n}$.

- a) Is h pre-image resistant?
- b) Is h strongly collision-free?

In each case give reasons for your answers.

[2] Consider the following hash function. It has as output an n vector whose entries lie in the range $0, \dots, k-1$ where k is a small integer (thus decimals if $k = 10$ and binary if $k = 2$). For any message M , the first n characters (converted to numerical values) are placed in the first row of a matrix A , the next n entries in M are placed in the second row and so forth until all of M has been used. Any remaining entries in the last row of A is padded with zeros if needed so that the length of the (possibly padded) message is m . Thus A is of size $\frac{m}{n} \times n$. Now select two small primes p and q . First, an n vector v_1 is produced by $v_1[j] \equiv \sum_j A_{ij} \pmod{p}$ and then an $\frac{m}{n}$ vector v_2 by $v_2[i] \equiv \sum_i A_{ij} \pmod{q}$. Thus v_1 and v_2 are column sums \pmod{p} and row sums \pmod{q} respectively. If $\frac{m}{n} < n$ then v_2 is extended to size n by setting $v_2[i + \frac{m}{n}j] = v_2[i]$ for $j = 1 \dots$ while if $\frac{m}{n} > n$ the last $\frac{m}{n} - n$ entries of v_2 are ignored. The hash function is now the n vector $h(M)_i \equiv v_1[i] + v_2[i] \pmod{k}$.

Which of the three properties does this function possess? You may assume that in an actual implementation n is quite large, say 160 bits if $k = 2$.

[3] In Alice's Elgamal signature scheme with private key a and public values $(p, \alpha, \beta \equiv \alpha^a \pmod{p})$, Eve chooses x and y with $\gcd(y, p-1) = 1$ and forms:
 $r \equiv \beta^y \alpha^x \pmod{p}$ and $s \equiv -ry^{-1} \pmod{(p-1)}$.

- a. Show that the pair (r, s) is a valid signature for the message $m = sx \pmod{(p-1)}$.

Note: m is likely to be a nonsensical message but Eve has a wide range of possibilities to select x and y in an attempt to construct a meaningful m . While hit-and-miss, the possibility is disturbing.

- b. Suppose that instead of signing the entire message a hash function is used and $h(m)$ rather than m itself is signed. Does this make it easier or more difficult to forge a signed message using this scheme?

[4] In the Elgamal signature scheme with private key a and public values $(p, \alpha, \beta \equiv \alpha^a \pmod{p})$, the signing equation is $s \equiv k^{-1}(m - ar) \pmod{(p-1)}$ with m the message, k a random integer with $\gcd(k, p-1) = 1$, $r \equiv \alpha^k \pmod{(p-1)}$.

If the signing equation is changed to $s \equiv a^{-1}(m - kr) \pmod{(p-1)}$ with $v_1 := \alpha^m \pmod{p}$ and $v_2 := \beta^s r^r \pmod{p}$, show that $v_1 \equiv v_2 \pmod{p}$ is a valid verification procedure.