VE475 Introduction to Cryptography
Homework 7

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

July 11, 2019

Homework 6

Ex. 5 - Merkle-Damgård construction

1. a) Since $f(0) = 0$ and $f(1) = 01$, $f(x_i)$ is always start with 0. So y can be separated into several segments start from 0, except for the first two digits. Those segments are injective with x_i, so the map s from x to y is injective.

   b) If z is empty, from what previous proved, there's no such x'. If z is not empty, since we have 11 at the beginning of y_{i+1}, so no this no such x' and z such that $s(x) = z \| s(x')$.

2. Because the previous conditions guarantee the mapping is collision resistant.

Homework 7

Ex. 1 - Cramer-Shoup cryptosystem

1. **Key generation:**

   - Alice generates a cyclic group G of order q with two distinct generators g_1, g_2. G could be $\mathsf{U}(\mathbb{Z}/p\mathbb{Z})$.
   - Alice chooses five random values (x_1, x_2, y_1, y_2, z) from $\{0, 1, \cdots, q-1\}$.
   - Alice computes $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, and $h = g_1^z$.
   - Alice publishes (c, d, h) and G, q, g_1, g_2 as her public key. She retains (x_1, x_2, y_1, y_2, z) as her private key.

   Encryption:

   - Bob converts plaintext into an element m in group G.
   - Bob chooses a random k from $\{0, 1, \cdots, q-1\}$, then calculates:
     - $u_1 = g_1^k$, $u_2 = g_2^k$.
     - $e = h^k m$.
     - $\alpha = H(u_1, u_2, e)$, where H is a collision-resistant cryptographic hash function.
     - $v = c^k d^{k\alpha}$.
   - Bob sends the ciphertext (u_1, u_2, e, v) to Alice.

   Decryption:

- Alice computes $\alpha = H(u_1, u_2, e)$ and verifies that

2.

3.

Ex. 2 - Simple questions

1.

2.

Ex. 3 - Birthday paradox

1.

2.

3.

4.

Ex. 4 - Birthday attack

1.

2.

3.

Ex. 5 - Faster multiple modular exponentiation

1.

2.

3.

4.