2007 - Exercises VI.

1. Show that an adversary Eve can break the Rabin cryptosystem if she has access to the decryption machine (but not the key).

2. (a) What is the probability that at least three students of the course IV054 have the same birthday?

   (b) What is the probability that at least one student of the course IV054 have the same birthday as you?

   (71 students attend IV054 course at this moment.)

3. Suppose $h : \{0,1\}^{2m} \to \{0,1\}^m$ is a strongly collision-free hash function. Let $h' : \{0,1\}^{4m} \to \{0,1\}^m$ be defined as

$$h'(x) = h(h(x_1)||h(x_2)),$$

   where x_1 is the first half of x and x_2 is the second half of x.

   Prove that h' is strongly collision-free.

4. None of the following definitions of secure encryption are correct (they do not express in sufficient detail what encryption is about). Find one or two errors in each of them.

   Let $Plaintexts, Keys, Ciphertexts$ be sets of strings of the same length over the same alphabet. Let $e : Plaintexts \times Keys \to Ciphertexts$ be an encryption function and $d : Ciphertexts \times Keys \to Plaintexts$ be a decryption function.

   (a) Let us denote $Plaintexts = \{P_1, .., P_n\}$. Let $\{q_i\}_i$ be a probability distribution on $Plaintexts$. For a given ciphertext C (which corresponds to a plaintext P) adversary knows that $P = P_i$ with probability q_i. Then (e, d) is a perfectly secure encryption scheme if $\{q_i\}_i$ is uniform.

   (b) Let $I(C, P)$ be mutual information between $C = e(P, K)$ and $P \in Plaintexts$ for some key K. Then (e, d) is perfectly secure encryption scheme if $I(C, P) = 0$ for all C and P.

   (c) Let $C = e(P, K)$ be a ciphertext for a plaintext P and a key K. Let $A : Ciphertexts \to Plaintexts$ be an algorithm. Then (e, d) is perfectly secure encryption scheme if $A(C) \neq P$.

5. Find all $x \in \mathbb{Z}_{209}$ such that $x^2 = 80 \bmod 209$. Explain (do not use brute force).

6. (a) Let p, q be distinct primes. Suppose that $x \equiv y \pmod{p}$ and $x \equiv y \pmod{q}$. Show that $x \equiv y \pmod{pq}$.

   (b) Let p, q be distinct primes and let $k \geq 0$ be an integer.
   Show that $x^{k(p-1)(q-1)+1} \equiv x \pmod{pq}$.

7. Are the following functions negligible? Explain your answer, you do not have to prove it.

   (a) $1/x!$

   (b) $1/\sqrt[5]{x}$

   (c) x^{-x}

   (d) $\sqrt[x]{x} - 1$

   (e) *(Bonus)*
   $1/f(x)$ where $f(x)$ = the number of people eating hamburgers in fast food restaurants and x being the amount of money that McDonalds' spends on advertisements.