IV054 Coding, Cryptography and Cryptographic Protocols

2017 - Exercises VI.

1. Consider the Rabin cryptosystem with $p = 43$ and $q = 47$.
   (a) Perform encryption of message $m = 2017$.
   (b) Determine all plaintexts that are mapped to the ciphertext from (a) by the Rabin encryption function.

2. Consider 66 students of IV054 are taking an exam and enter a room one by one. The first student who has the same birthday as someone who has already entered the room will automatically receive the grade A. Which one is most likely to be the first, *i.e.* which position would you prefer?

3. Decide whether the following statement is true:

   Let $h : \{0,1\}^n \to \{0,1\}^m$ be a strongly collision resistant hash function and let $h' : \{0,1\}^n \to \{0,1\}^{m+1}$ be defined in the following way:

   $$h'(x) = (1.h(x)) \oplus (h(x).0),$$

   where $a.b$ denotes the concatenation of strings a and b. Then h' is also strongly collision resistant hash function.

   Prove your answer.

4. Consider the Rabin cryptosystem with $n = 11573$. You have found out that cryptotext $c = 879$ can be decrypted as $m_1 = 155$ and $m_2 = 1149$. Show that with this information you are able to decrypt any message.

5. Consider a two-round Feistel scheme with the round function being one-time pad with the respective keys being $K_0 = 110$ and $K_1 = 100$. Decrypt the cryptotext 001000.

6. Determine all odd quadratic residues modulo 2^n for $n \geq 3$, *i.e.* odd numbers k such that

   $$x^2 \equiv k \pmod{2^n}$$

   has a solution for $x \in \mathbb{Z}$.
   (a) Find all odd quadratic residues modulo 8.
   (b) Show that for $n > 3$, the congruence $x^2 \equiv k \pmod{2^n}$ has either zero or exactly four solutions for $x \in \mathbb{Z}$.

   Hint: You can use without proof the fact that for $n > 3$, any odd positive integer $m < 2^n$ satisfies the congruence $m \equiv (-1)^{e_1} 5^{e_2} \pmod{2^n}$ for a unique $e_1 \in \{0,1\}, e_2 \in \{0,1,\ldots,2^{n-2}\}$.

   (c) Using (a) and (b), describe all odd quadratic residues modulo 2^n for $n > 3$ by a single congruence.