

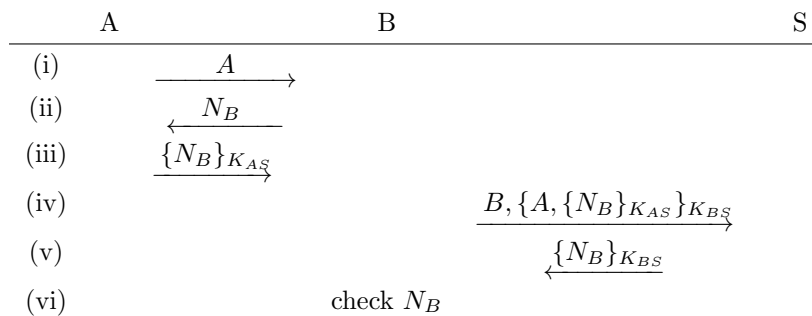
IV054 Coding, Cryptography and Cryptographic Protocols  
 2012 - Exercises IX.

1. Let  $G$  be a cyclic group of prime order  $p$  and let  $g$  be its generator. Alice's private is some  $x < p$  and her public key is  $X = g^x$ . Consider the following user identification scheme:
  - Alice randomly chooses  $r < p$  and sends  $R = g^r$  and  $S = g^{x-r}$  to Bob.
  - Bob responds by sending a randomly chosen bit  $b$ .
  - If  $b = 0$ , Alice sends  $z = r$  to Bob, otherwise she sends  $z = x - r$ .
  - (a) Find and explain the acceptance condition.
  - (b) Show that the adversary Eve is able to impersonate Alice with probability  $\frac{1}{2}$ .
  - (c) Propose a change which makes the protocol more secure.
2. Consider the Shamir's  $(5, 3)$ -threshold secret sharing scheme with  $p = 211$ . Participants  $P_1, P_2$  and  $P_3$  with shares  $(1, 171), (2, 46)$  and  $(3, 170)$  want to reconstruct the secret. Show in detail their computation.
3. Let  $h_1, h_2$  be hash functions with the same length of outputs such that one of them is strongly collision-free. Use them to find a strongly collision-free hash function  $h$ . Show that your function has the desired property.
4. Suppose you are an army cryptographer. Your mission is to design a secret sharing scheme allowing one General and one Lieutenant General or five Lieutenant Generals to fire a missile. Accomplish your mission.
5. There are four persons in a room, and one of them is a foreign spy. Other three persons share a secret using the Shamir's threshold scheme with  $p = 11$ . Any two of them can recover the secret. The foreign spy chooses his share randomly. Together with the secret sharing participants, the four shares are as follows:

$$P_A : (1, 7), \quad P_B : (3, 0), \quad P_C : (5, 10), \quad P_D : (7, 9)$$

Find out who is the foreign spy and calculate the secret.

6. Consider the following authentication protocol:



In the protocol, an entity  $A$  authenticates herself to another entity  $B$  with the help of an authentication server  $S$ . We denote a secret key shared by entities  $X$  and  $Y$  by  $K_{XY}$ , and let  $N_X$  denote a random value generated by  $X$  freshly for each instance of the protocol. The encryption of a message  $m$  by a key  $K$  is denoted  $\{m\}_K$ .

- (a) Show that a malicious user  $M$  can impersonate  $A$  to  $B$  without any contribution from  $A$ .
- (b) Propose a corrected version of the protocol.

7. Suppose Alice and Bob share a random secret key and they want to use it to authenticate their messages  $0 \leq m \leq 32$ . To authenticate a message  $m$  with a 2-bit tag  $t$ , Alice chooses two numbers  $0 < q < 37$  and  $0 \leq r < 37$  according to the shared key, computes a hash of  $m$ :

$$t = ((qm + r) \pmod{37}) \pmod{4}$$

and sends  $(m, t)$  to Bob.

Bob receives a possibly modified pair  $(m', t')$  and computes  $t_b = ((qm' + r) \pmod{37}) \pmod{4}$ . If  $t_b = t'$ , he accepts.

- (a) What is the probability of successful mounting an impersonation attack?
- (b) What is the probability of successful mounting a substitution attack?