

**Cryptography 2 (2XC13)/Cryptographic Protocols 1 (2WC17)**  
**Exam, April 17, 2014, 2:00–5:00pm**

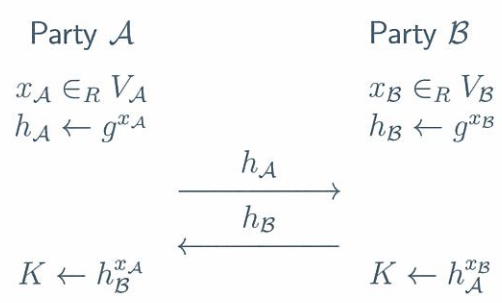
Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.

Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

- 1) Let  $\langle g \rangle$  be a cyclic group of large prime order  $n$ .  
 Consider the following parameterized Diffie-Hellman key exchange protocol:



Let distributions  $X$  and  $Y$  be given by:

$$X = \{g^t : t \in_R \mathbb{Z}_n^*\},$$

$$Y = \{g^u : u \in_R \mathbb{Z}_n\}.$$

Let  $\Delta$  denote statistical distance.

- a) Determine  $\Delta(K; X)$  if  $V_A = \mathbb{Z}_n^*$  and  $V_B = \mathbb{Z}_n^*$ .
- b) Determine  $\Delta(K; X)$  and  $\Delta(K; Y)$  if  $V_A = \mathbb{Z}_n$  and  $V_B = \mathbb{Z}_n^*$ .
- c) Determine  $\Delta(K; Y)$  if  $V_A = \mathbb{Z}_n$  and  $V_B = \mathbb{Z}_n$ .

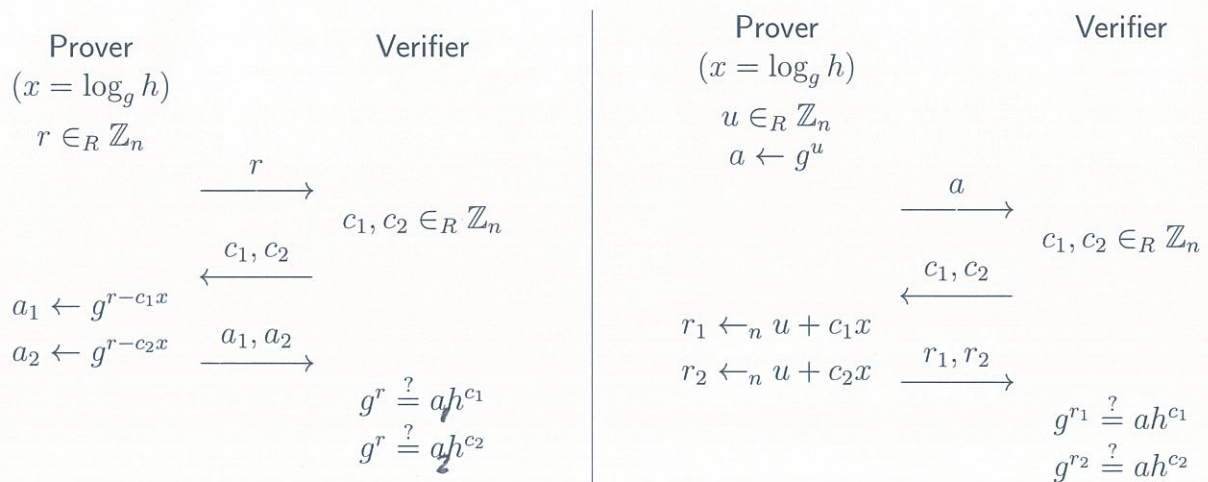
- 2) Let  $\langle g \rangle$  be a cyclic group of large prime order  $n$ .  
 Show that each of the following computational problems is random self-reducible.

- a) Given  $g^x, g^y, g^{xy}$ , compute  $g^{\frac{1}{xy}}$ , where  $x, y \in \mathbb{Z}_n^*$ .
- b) Given  $g^x, g^y$ , compute  $g^{(x-1)/y}$ , where  $x \in \mathbb{Z}_n$  and  $y \in \mathbb{Z}_n^*$ .

- 3) Let  $\langle g \rangle$  be a cyclic group of large prime order  $n$ . Let  $h \in \langle g \rangle$  denote a random group element such that  $\log_g h$  is unknown to anyone. Consider relation  $R$ :

$$R = \{(A, B, C; x, y) : A = g^x \wedge B = g^y \wedge (C = h^x \vee C = h^y)\}.$$

- a) Give a  $\Sigma$ -protocol for relation  $R$  and show that it is complete, special sound, and special honest-verifier zero-knowledge.
- b) Let  $H$  be a cryptographic hash function. Turn your  $\Sigma$ -protocol into a non-interactive  $\Sigma$ -proof (using the Fiat-Shamir heuristic) and show how the  $\Sigma$ -proof is verified.
- 4) Let  $\langle g \rangle$  be a cyclic group of large prime order  $n$ . Consider the following two protocols as variations of the Schnorr  $\Sigma$ -protocol for relation  $\{(h; x) : h = g^x\}$ :



- a) Show that both protocols are complete.
- b) For each of the protocols determine if it is special sound. If so, provide a proof; otherwise, show why not.
- c) For each of the protocols determine if it is special honest-verifier zero-knowledge. If so, provide a proof; otherwise, show why not.

1a: 3	1c: 3	2a: 6	3a: 11	4a: 2	4c: 5
1b: 6		2b: 6	3b: 3	4b: 5	

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5 (for 2XC13) and rounded to an integer (for 2WC17).