

Modern Cryptology (236506) – Exercise no. 5

Submission in singles on 1/7/2005, 12:00 (or after the exam) to Box #96 floor 5

5 bonus points will be given to printed (or exceptionally clear and organized) submissions.

Explain all your answers.

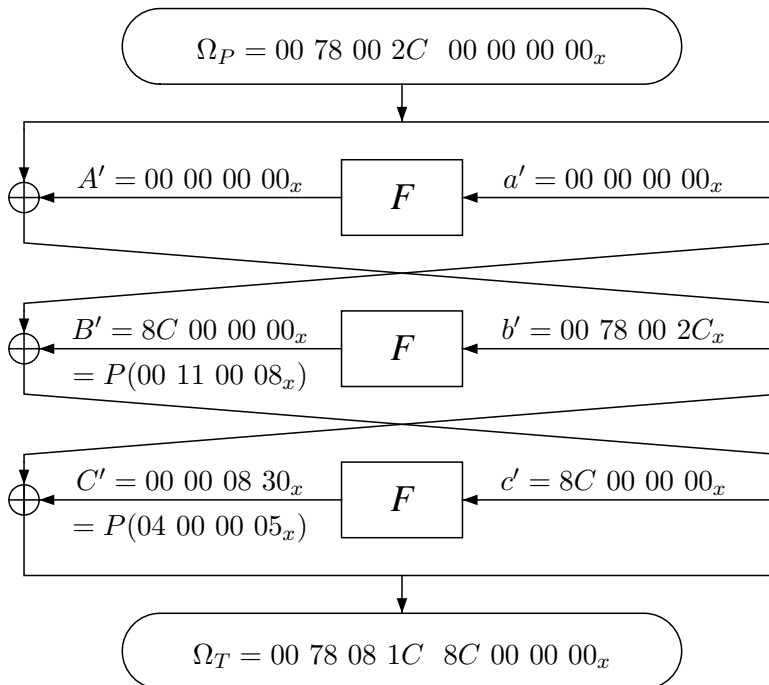
1. A student that studied Zero-Knowledge wondered if a security proof using a simulator indeed proves security. He suspected that it is possible to prove that a protocol is Zero-Knowledge, while in fact, the protocol leaks information. To test his suspicions, he suggested the following change to the $G3C$ protocol shown in class: The prover would be identical to the original prover, but if the verifier asks for an edge $(u_j, u_k) \notin E$, the prover opens the commitment for these vertices (rather than calling the verifier a cheater). Therefore, this prover will be referred to as *frayer prover*.
 - (a) Given that the coloring is unique (up to its 6 permutations), show a cheating verifier that learns the 3-coloring within $2|E|$ iterations of the protocol. Therefore, this verifier will be referred to as *tachman verifier*.
 - (b) Show that the transcript of the original verifier and the frayer prover is identical to the transcript of the original verifier and the original prover (and therefore, it is polynomially indistinguishable from the one received by the original simulator).
 - (c) Since the tachman verifier runs $2|E|$ iterations, the transcript length is $2|E|$ iterations of the protocol. Is there an averaged polynomial-time Turing machine that can distinguish a transcript of the tachman verifier with original simulator, to a transcript of an execution of the protocol between the tachman verifier with the frayer prover? Explain.
 - (d) Let T be a transcript of an execution of the protocol between the tachman verifier and the frayer prover; let S be some simulator, and T' the transcript of S with the tachman verifier. Assuming that the simulator cannot solve the $G3C$, show a polynomial-time algorithm that distinguishes between T and T' (i.e., show an algorithm that given T outputs “Real” with high probability, and when given T' outputs “Simulator”).
 - (e) Is the protocol using the original prover a ZK protocol and is protocol using the frayer prover a ZK protocol?
2. When planning a system of a nuclear missile launch we would like to make sure that a single lunatic will not be able to launch a missile. We would prefer that two lunatics will not be able to do so, as well. We would like that at least three out of five colonels will be crazy enough to permit a launch. It was decided to use an $(3, 5)$ -secret sharing scheme where five colonels receive shares of the launch password S .

Three colonels Alice, Bob and Carol are sitting inside the bunker when a launch order is received directly from the prime-minister (who is the only single lunatic authorized to order a launch). Two of the colonels reveal their true shares, but the third, who is interested in stopping the launch, reveals a false share. Therefore when the three colonels reconstruct the secret they get a false secret S' .

- (a) Prove that given the three shares an honest colonel cannot discover which of the other two is to blame for the failed launch.
 - (b) It turns out that the above launch order was an exercise designed to test the missile launch system. As Alice, Bob and Carol reconstructed a false secret a military police investigator (who has no knowledge of S) arrives at the base. and interrogates all five colonels. Explain how can the investigator find the guilty colonel.
 - (c) Propose a modification of the system to prevent this kind of cheating. Your suggestion should ensure that each coalition of less than three colonels will have **no information** on the secret. Hint: Bit commitment might prove useful.
3. (Bonus: 7 points) Compute the difference distribution table of the Byte Substitution of Rijndael. What are the 5 highest entries and their probability? (The byte substitution is available online on the course's site).

Note that you are not required to submit the entire difference distribution table (and doing so, you kill too many trees!).

4. Compute the probability of the following 3-round characteristic:



5. Consider DES reduced to four rounds, and assume that the two pairs P_1, P_1^* ($P_1 \oplus P_1^* = \Omega_P$), P_2, P_2^* ($P_2 \oplus P_2^* = \Omega_P$) are right pairs with respect to the characteristic of question 4. Recover at least 14 *bits of information* on the subkey of the fourth round (it is possible to

find 28 bits of information from the following data, but you are required to find 14), given:

P_1	=	46 03 1E 01 88 D3 C2 73 _x
P_1^*	=	46 7B 1E 2D 88 D3 C2 73 _x
T_1	=	02 55 6F 8D 0E DD D8 90 _x
T_1^*	=	39 21 67 E9 0E A5 D0 8C _x
T_1'	=	3B 74 08 64 00 78 08 1C _x
P_2	=	F8 3B CB 26 76 11 03 58 _x
P_2^*	=	F8 43 CB 0A 76 11 03 58 _x
T_2	=	4A 1D 6B 75 22 E2 49 11 _x
T_2^*	=	43 1A 47 79 22 9A 41 0D _x
T_2'	=	09 07 2C 0C 00 78 08 1C _x
$P^{-1}[3B 74 08 64_x]$	=	00 2A DA 5D _x
$P^{-1}[09 07 2C 0C_x]$	=	00 60 C5 2B _x
$P^{-1}[B7 74 08 64_x]$	=	00 3B DA 55 _x
$P^{-1}[85 07 2C 0C_x]$	=	00 71 C5 23 _x

Explain your answer. (You can find an online version of the difference distribution tables and list of pairs on the course homepage, also note that we gave a few hopefully useful values of P^{-1})