INTRODUCTION TO MODERN CRYPTOGRAPHY
KU BLOCK 1A, 2016-17

HOMEWORK 4
DUE: TUESDAY 1/11/2016 8:30AM

GORJAN ALAGIC

Instructions.

- Collaboration is encouraged, but each student *must* understand and write up their own solution set entirely by themselves.
- All answers must be accompanied by complete and clearly explained proofs. A correct answer with no explanation will receive a zero score.
- Your goal in proofs is to convince *me* that your answer is correct, and that you understand why it is correct. It is difficult to do this without words. As in all writing, these words should almost always come in complete sentences.
- For open-ended (e.g., yes/no) questions, think carefully about what constitutes a "proof" that your response is correct. Sometimes, all it takes is a counterexample.
- If you are using a theorem proved in class, indicate it clearly by name (or just restate it.) Theorems from outside class are ok to cite, so long as they are not about cryptography. If you want to use a theorem from cryptography, you have to include the proof.

Problems.

(1) Work two complete examples of the Diffie-Hellman key exchange protocol, using (i.) prime $p = 31$ and generator $g = 3$, and (ii.) prime $p = 23$ and generator $g = 5$. Choose "random" (but interesting) values for the randomness of Alice and Bob. Specify each step clearly: who performs the step, what they send to the other party, etc. Be sure to also check that Alice and Bob get the same key in the end.

(2) Describe a "man-in-the-middle" attack on the Diffie-Hellman key exchange protocol (taking place over an unauthenticated channel.) At the end of your attack, the active adversary should share a key k_A with Alice and a different key k_B with Bob, without either Alice or Bob realizing it.

(3) Work a complete example of El Gamal encryption, using $p = 29$ and $g = 2$. Choose "random" (but interesting) values for the rest. Start with key generation, and write down the public and private keys explicitly. Then have Bob send the plaintext 25 and show how to encrypt and decrypt it correctly.

(4) Describe an active attack on El Gamal encryption (taking place over an unauthenticated channel), where the adversary can (i.) decrypt all the sender's messages, and (ii.) send plaintexts of the adversary's choice to the receiver. Once again, neither the sender nor the receiver should notice the attack.

(5) Prove that public-key encryption with perfectly indistinguishable encryptions (i.e., perfect security) is impossible.

Department of Mathematical Sciences, University of Copenhagen
E-mail address: galagic@gmail.com