Topics in Discrete Mathematics - Cryptography
Problem Sheet 2

Daniel P. Martin

University of Bristol 2018-2019

1 RSA

Question 1. Upon running the Key Generation algorithm for RSA the two primes chosen are $7, 11$ and e is chosen to be 13. Calculate, all the values computed by the key generation algorith. Use this information to encrypt the message $m = 47$ and to decrypt the ciphertext $c = 73$.

Question 2. Alice and Bob have public keys of the form (N, e_1) and (N, e_2) respectively, so that they use the same public modulus. Suppose that e_1 and e_2 are coprime. Show that we can easily decrypt any message that is sent to both Alice and Bob (if the two corresponding ciphertexts are intercepted).[1]

2 ElGamal

Question 3. For this question consider the multiplicative group $\mathbb{Z}_{283}$ and the generator $g = 60$ meaning that we are working in a multiplicative subgroup with order $q = 47$. Given Bob has private key $x = 7$, calculate his public key h. Assume Alice has message $m = 101$ and chooses $r = 36$, compute the corresponding ciphertext.

Question 4. An encryption scheme is called one way if given an encryption c of some message m, it is hard to learn m without the secret key.

Show that, for ElGamal on group $\mathbb{G}$, if it is possible to learn m given a ciphertext c then it is possible to solve the CDH problem in the group $\mathbb{G}$

Question 5. Consider the following scenario: if an adversary can submit a chosen message m, and receives either an encryption of m or of a random message r. An encryption scheme is called Real or Random secure under chosen plaintext attack, if the adversary can not tell which ciphertext they have.

Show that, for ElGamal on group $\mathbb{G}$, if it is possible to break the real or random security, then it is possible to solve the DDH problem in the group $\mathbb{G}$.

---

[1] Many thanks to Dan Fretwell for this nice question.