Esecurity: secure internet & e-voting, summer 2013

MICHAEL NÜSKEN

10. Exercise sheet
Hand in solutions until Monday, 24 June 2013, 08:00

Exercise 10.1 (Features of ElGamal encryption). (16+2 points)

ElGamal encryption works in a finite group $G = \langle P \rangle$ (which we write additively here) with some generator P. Bob generates a private key b and computes his public key $B = bP$. Enryption of a message $M \in G$ is performed by picking a temporary secret $t \in \mathbb{Z}_{\#G}$ and computing $(tP, M + tB)$. Bob decrypts (T, X) by computing $M' = X - bT$.

(i) Prove correctness. 2

(ii) Given two different messages M_1, M_2. Show that deciding whether (T, X) is an encryption of M_1 is equivalent to solving a decisional Diffie-Hellman problem. 4

(iii) In other words: ElGamal encryption is IND-KO secure if and only if DDH is hard in G. 3

(iv) Assume that for $i = 1, 2$ the ciphertext (T_i, X_i) is an ecnryption of a message M_i. Show that $(T_1 + T_2, X_1 + X_2)$ is an encryption of $M_1 + M_2$. 3

(v) Conclude that ElGamal encryption is not IND-CCA secure. You may obtain the bonus points if you achieve this by calling the CCA oracle only once. 4+2

Exercise 10.2 (Bits of history). (10 points)

Look up some bits of the history of voting technology.

(i) What was the 'gabinia lex'? When were they used? 2

(ii) When have secret elections been introduced? 2

(iii) When did paper ballots (aka. Australian ballot) replace oral ballots? 2

(iv) What are Lever voting machines, when and where were they used? What are their most prominent pros and cons? 4