CSCI 476 Computer Security

Exercise for Chapter 2 & 3.

(a) A bank wants to store the account number of its customers (an 8-digit number) in encrypted form on magnetic stripe ATM cards. Discuss the security of the following methods for storing the account number against an attacker who can read the magnetic stripe: (1) store a cryptographic hash of the account number; (2) store the ciphertext of the account number encrypted with the bank's public key using a public-key cryptosystem; (3) store the ciphertext of the account number encrypted with the bank's secret key using a symmetric cryptosystem.

(b) If a password is salted with a 32-bit random number, how big is the dictionary attack search space for a 500,000 word dictionary?