# Dept. of Computer Science and Engineering, National Sun Yat-sen Univ.

## First Semester of 2021 PhD Qualifying Exam

**Subject: Cryptography**

**Problem 1: (each 5 points) (a) Prove that a permutation $\pi$ in the Permutation Cipher is an involutory key if and only if $\pi(i) = j$ implies $\pi(j) = i$, for all $i, j \in \{1, ..., m\}$. (b) Determine the number of involutory keys in the Permutation Ciphjer for $m = 2, 3, 4, 5$, and $6$.**

**Problem 2: (10 points) Let $\mathcal{P} = \{a, b\}$ and let $\mathcal{K} = \{K_1, K_2, K_3, K_4, K_5\}$. Let $\mathcal{C} = 1, 2, 3, 4, 5$, and suppose that the encryption functions are represented by the following encryption matrix.**

| | $a$ | $b$ |
|---|---|---|
| $K_1$ | 1 | 2 |
| $K_2$ | 2 | 3 |
| $K_3$ | 3 | 1 |
| $K_4$ | 4 | 5 |
| $K_5$ | 5 | 4 |

**Now choose two positive real numbers $\alpha$ and $\beta$ such that $\alpha + \beta = 1$, and define $\Pr[K_1] = \Pr[K_2] = \Pr[K_3] = \alpha/3$ and $\Pr[K_4] = \Pr[K_5] = \frac{\beta}{2}$.**
**Prove that this cryptosystem achieves perfect secrecy.**

**Problem 3: (10 points) Let $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem. Then $H(\mathbb{K}|\mathbb{C}) = H(\mathbb{K}) + H(\mathbb{P}) - H(\mathbb{C})$.**

**Problem 4: (10 points) Please prove formally the extended Euclidean algorithm.**

**Problem 5: (10 points) Please prove formally the Chinese Remainder Theorem.**

**Problem 6: (10 points) Please define a Digital Signature Algorithm (DSA) formally and show that in which case DSA will be easy for an adversary to compute the secret key easily. (Note: Please also state how the variables are selected when defining DSA.)**

**Problem 7: (10 points) We give yet another protocol failure involving the RSA Cryptosystem. Suppose that three users in a network, say Bob, Bart, and Bert, all have public encryption exponents $b = 3$. Let their moduli be denoted by $n_1, n_2, n_3$, and assume that $n_1, n_2$, and $n_3$, are pairwise relatively prime. Now suppose Alice encrypts the same plaintext $x$ to send to Bob, Bart, and Bert. That is, Alice computes $y_i = x^3 \mod n_i, 1 \leq i \leq 3$. Describe how Oscar can compute $x$, given $y_1$, $y_2$, and $y_3$, without factoring any of the moduli.**

**Problem 8: (15 points) Please prove formally the security of RSA-based full domain hash scheme. (Note: Please derive that the probability of breaking the scheme is negligible step by step.)**

**Problem 9: (15 points) Suppose there are three entities A, B, and C, where B and C are fully trusted, and the communication channel between them is secure. Moreover, A and C share a secret key, $K$. Please design a three-party authenticated key exchange protocol with forward secrecy using only symmetry-based encryption, cryptographic hash function, and Diffie-Hellman key agreement. (Note:The security feature of mutual authentication, session key exchange, and forward secrecy should be achieved among A and B).**