**CNS Homework2**

姓名: 徐有慶

學號: r05922162

**Handwriting:**

1. **Encryption Algorithms:**

**Differences:**

* Symmetric cryptography只需要一個shared secret key即可，Asymmetric cryptography則需要public和private key
* Shared secret key只有要溝通的雙方可以知道，而public key可以被全部的人知道，private key則只有擁有者知道

**Example:**

Symmetric cryptography:

* DES
* AES

Asymmetric cryptography:

* RSA
* ElGamal

**To achieve higher security, which method usually needs a larger key?**

Asymmetric cryptography needs a larger key

因為Asymmetric cryptography在public key的部分是公開的，若是產生方法的key很簡單或是key的長度不夠長的話，可能很容易就被別人給破解，只好靠增加key的大小來提升破解的難度。

**Which method is generally faster, why?**

Symmetric cryptography is generally faster

如上面所說，Asymmetric cryptography需要較大的key，計算量也相對較大，所以速度就會比較慢。

1. Three-way Diffie-Hellman

A -> B: ga mod p

B -> C: gab mod p

C -> B: gc mod p

B -> A: gbc mod p

1. ElGamal threshold decryption

**Capture The Flag:**