

CAS CS 538. Problem Set 4

Problem 1. Consider the following symmetric encryption scheme: Alice and Bob agree on a large prime p . Now, to encrypt a message m encode it as a large prime¹ p_m and use $c = p \cdot p_m$ as the ciphertext. Decryption of ciphertext c is obvious: $p_m = c/p$ (and then decode m from p_m).

Below, use p_m as the plaintext (thus avoiding the encoding/decoding issue).

- (a) Show that the Factoring Assumption implies that this encryption scheme is secure.
- (b) Show that this encryption is insecure if the same key is used for more than one encryption.

Problem 2. This problem gives an example of what's wrong with deterministic encryption. Below assume we use a simple Rabin encryption, but suppose the messages are sufficiently long (so the attack we mentioned in the class does not work).

(a) Suppose Bob and David have two independent Rabin public keys n_B and n_D , respectively. Suppose Alice has a single message m to send to both of them, and m is a square in both $\mathbb{Z}_{n_B}^*$ and $\mathbb{Z}_{n_D}^*$. She encrypts it with plain-Rabin twice to get $c_B = m^2 \bmod n_B$ and $c_D = m^2 \bmod n_D$. Show how an eavesdropper Eve who intercepts c_B and c_D can recover m . (Hint: if Rabin public keys are generated independently, then they are relatively prime with all but negligible probability. You can use the fact that Chinese remainder theorem applies not only to primes, but to any pair of relatively prime integers.)

(b) *Extra credit* Generalize this attack for a small public exponent RSA encryption. How many moduli would Alice need to encrypt m for to make the attack successful for public exponent 3? 5?

Problem 3. In this problem, we will see how powerful hybrid arguments can be.

A commonly used practical way to encrypt long messages is to use public key encryption to encrypt a symmetric encryption key s and then use s to encrypt the message. Since pseudo-random one-time pad is still our only symmetric cipher so far, this yields the following scheme:

Let (Gen, E, D) be a GM-secure multi-bit public-key cryptosystem, and let G be a pseudorandom generator. Consider the following public-key cryptosystem. To encrypt m of length l , select a random seed s , generate $p = G(s)$ of length l , and output $c = \langle E_{\text{PK}}(s), p \oplus m \rangle$. Show that this cryptosystem is also GM-secure. Suggestion:

- (a) Show that $\langle E_{\text{PK}}(s), G(s) \rangle$ is indistinguishable from $\langle E_{\text{PK}}(s), R \rangle$, where $R \in_R \{0, 1\}^l$. Hint: use a hybrid argument, with $E_{\text{PK}}(s), G(t)$, for a random unrelated t , as a hybrid point.
- (b) Show that $\langle E_{\text{PK}}(s), p \oplus m_0 \rangle$ is indistinguishable from $\langle E_{\text{PK}}(s), p \oplus m_1 \rangle$. Hint: use a hybrid argument, with two hybrid points, and the previous part.

Problem 4. Ex. 3.4 (pg.106)

Problem 5. Ex. 3.10 (pg.107)

¹The encoding of a message m into a prime p_m can be for example as follows: concatenate ASCII codes of all the characters of the message m (terminating with a special "end of message" token) to obtain a large number. Add a few more bits to make the resulting number into a prime (this can be done by trying different suffixes of a small number of bits and testing the resulting number for primality) — it turns out that this can actually be reasonably efficient.