- **Assignment 2: Task 3**
- This time you have to use LaTeX to prepare your answer document. Submit a pdf file generated using pdflatex. LaTeX is the standard document preparation system used in the academic community. This will give you an opportunity to pick up some basic LaTeX skills. You will see how writing Mathematical text is so much easier.
- Deadline: 2nd April (Submit at the beginning of the class. You lose 3 point per day for late submissions.)

There are 3 questions for a total of 15 points.

---

(4) 1. Consider the CBC$ encryption discussed in class. Prove the following theorem (this was discussed partially in the class):

Theorem 1. *Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $SE = (E, D)$ be the corresponding CBC$ encryption scheme. Let A be an IND-CPA adversary that runs in time t and makes q queries totaling σ blocks. Then there is a PRF adversary B against E such that:*

$$Adv_{ind-cpa}(A, SE) \leq 2 \cdot Adv_{PRF}(B, E) + \frac{\sigma^2}{2^n}$$

Moreover, B makes at most σ oracle queries and has a running time $t + \theta(\sigma \cdot n)$.

2. *(This problem has been borrowed from a course on Cryptography at Princeton University taught by Boaz Barak)*

Consider the following symmetric encryption scheme $SE = (E, D)$ that uses key of size n bits and encrypts messages of size $3n$ bits. Note that in the description below $G : \{0,1\}^{n+l} \to \{0,1\}^{3n+32}$ is a pseudorandom generator and $CRC : \{0,1\}^{3n} \to \{0,1\}^{32}$ is some checksum function (you may consider this to be the IEEE CRC-32 function).

$E_K(M)$

- Pick $R \in \{0,1\}^l$ uniformly at random.
- Output $R||(G(R||K) \oplus (M||CRC(M)))$

$D_K(C)$

- Parse C as $R'||C'$.
- $M'||T' \leftarrow G(R'||K) \oplus C'$
- If $(CRC(M') \neq T')$ output *failure* else output M'.

Show the following:

(1) (a) Show that for every pseudorandom generator G, the above scheme is not IND-CPA secure against adversaries running in time $2^{l/2} \cdot poly(n)$.

(2) (b) Show that for every pseudorandom generator G, the above scheme is not IND-CCA secure.

(3) (c) Show that *there exists* a secure pseudorandom generator G for which the above scheme is not even IND-CPA secure w.r.t. polynomial-time adversaries.

All of these results seem to indicate that the above encryption scheme is not very good. Nevertheless this is basically the encryption scheme used for the Wi-Fi encryption protocol WEP (for Wired Equivalent Privacy) IEEE 802.11b standard. After completing this exercise, read about the various ways in which WEP has been broken. You will find more than enough material on this on the web.

(5) 3. You have to design an algorithm to multiply two $n \times n$ matrices A and B. The matrices contain m-bit numbers. Note that brute-force multiplication will have a running time of $O(n^3 \cdot m^2)$. Use Chinese Remaindering Theorem to improve the running time to $O(n^3 \cdot m + n^2 \cdot m^2)$.