Homework 3

1 Problem 1 (5 points)

In class, we saw the birthday paradox: if we select q random integers $x_1, \ldots, x_q$ from a list of size n with replacement, the probability two of the x_i will be equal is $O(q^2/n)$.

Here we consider a generalization of this problem. Fix an integer $k > 2$. Show that the probability that some subset of k of the x_i are equal is $O(q^k/n^{k-1})$.

2 Problem 2 (10 points)

Two standards committees propose to save bandwidth by combining compression (such as the Lempel-Ziv algorithm used in the zip and gzip programs) with encryption. Both committees plan on using a variable length secret key encryption scheme.

(a) One committee proposes to compress messages before encrypting them. Explain what might go wrong.

(b) The other committee proposes to compress ciphertexts after encryption. Explain what might go wrong.

Over the years many problems have surfaced when combining encryption and compression. The CRIME and BREACH attacks are good representative examples.

3 BONUS Problem 3 (5 points)

Let $G : \{0,1\}^\lambda \to \{0,1\}^n$ be a PRG with $\lambda < n$. We can use G to get a stream cipher $\mathsf{Enc}(k, m) = G(k) \oplus m$. We saw in class that if the PRG is a secure pseudorandom generator, then Enc has ciphertext indistinguishability (in the one-time setting)

Prove the converse: if $\mathsf{Enc}(k, m) = G(k) \oplus m$ has ciphertext indistinguishability, prove that G *must* be a pseudorandom generator.

4 Problem 4 (35 points)

Consider the following notions of security for encryption schemes.

(i) **Left-or-Right (LoR) Indisitnguishability.** This is the notion of security we saw in class

(ii) **Real-or-Random Plaintext (RoRP) Indistinguishability.** This security notion is defined by the following experiment. The adversary makes polynomially-many queries to the challenger on messages m in the message space. The challenger responds to the queries as follows. If its input bit is $b = 0$, then the challenger encrypts m to get a ciphertext c, which it returns to the adversary. If the challenger's input bit is $b = 1$, then the challenger chooses a new random message m' and encrypts m' to get a ciphertext c, which it then returns to the adversary. Security is defined in the usual way: a scheme has RoRP indisitnguishability if, for all adversaries A running in polynomial time, there is a negligible function ϵ such that A's advantage in the RORP experiment is at most $\epsilon(\lambda)$.

(iii) **Real-or-Random Ciphertext (RoRC) Indistinguishability.** This security notion is defined by the following experiment. The adversary makes polynomially-many queries to the challenger on messages m in the message space. The challenger responds to the queries as follows. If its input bit is $b = 0$, then the challenger encrypts m to get a ciphertext c, which it returns to the adversary. If the challengers input bit is $b = 1$, then the challenger chooses a random string c in the ciphertext space C, which it then returns to the adversary. RoRC security is defined in the natural way.

(iv) **Real-or-Zero (RoZ) Indistinguishability.** This security notion is defined by the following experiment. The adversary makes polynomially-many queries to the challenger on messages m in the message space. The challenger responds to the queries as follows. If its input bit is $b = 0$, then the challenger encrypts m to get a ciphertext c, which it returns to the adversary. If the challengers input bit is $b = 1$, then the challenger encrypts $m' = 0$ to get a ciphertext c, which it

Some of these notions are equivalent (in the sense that if $(\mathsf{Enc}, \mathsf{Dec})$ satisfies one notion, then it must also satisfy the other), and some are stronger than others (in the sense that if $(\mathsf{Enc}, \mathsf{Dec})$ satisfies notion (a), it must satisfy notion (b), but there are examples of schemes that satisfy (b) but not (a)). Your goal is to figure out the relationships between each of these security notions.

Your solution will contain several proofs of statements of the form: "if $(\mathsf{Enc}, \mathsf{Dec})$ satisfies notion (a), then it also satisfies notion (b)" (this can succinctly be stated as "notion (a) implies notion (b)"). Note that you do not necessarily need to prove all implications: if notion (a) implies notion (b) and notion (b) implies notion (c), then you can conclude without proof that notion (a) also implies notion (c).

Your solution will also contain some proofs of statements of the form: "There exist $(\mathsf{Enc}, \mathsf{Dec})$ satisfying notion (a) but that does not satisfy notion (b)" (this can be succinctly stated as notion (a) does not imply notion (b)). For these kind of statements, you may assume as a starting point a secure PRG, a secure PRF, or an encryption scheme that is guaranteed to satisfy any of the notions above (LoR, RoRP, RoRC,RoZ), which you then use to build your $(\mathsf{Enc}, \mathsf{Dec})$ counter example.

Again, note that you do not necessarily need to prove all implications. For example, if (a) does not imply (b), but (c) does imply (b), then you can conclude without proof that (a) does not imply (c).

There are a total of 12 statements to decide on (for every pair of notions (a) and (b), you must decide whether or not (a) implies (b) and whether or not (b) implies (a)). As a hint, it is possible to select 5 statements, prove those, and then derive the remaining 7 from these 5. You will not be penalized or rewarded based on the number of statements you prove; if you prove all 12 directly, that is fine (though it will be more work on your part).