Exercise Sheet 11

Cryptography and Security 2022

Exercise 1 Distribution of Birthdays

This semester, we had $M = 81$ registered students.[1] We assume their birthdays are *a priori* uniformly distributed and independent, in a calendar of $N = 365$ days. (Indeed, no student is born on a February 29). In what follows, the *a priori* probabilities refers to the situation *before* we look at the actual birthdays (which we will do in 5).

1. What was the *a priori* probability that a given student is born on a January 22?
2. What is the *a priori* probability that your right neighbor shares with you the same birthday? (Consider the left neighbor if you have no right neighbor.)
3. For a given student, what is the *a priori* probability that there are *exactly* two others students in the class sharing the same birthday with him?
4. What was the *a priori* expected number of unordered pairs of different students with the same birthday? Do the same for unordered triplets of students.

   HINT: the number of pairs of students with the same birthday is

   $$\sum_{\text{pair}} 1_{\text{the students in pair share the same birthday}}$$

5. We observed

   - 3 students are born on a March 2,
   - 3 students are born on a May 5,
   - 3 students are born on a July 4,
   - 2 students are born on a April 14,
   - 2 students are born on a May 9,
   - 2 students are born on a June 2,
   - 2 students are born on a June 13,
   - 2 students are born on a August 5,
   - 2 students are born on a November 1,
   - 60 students have a unique birthday.

   From the observation, how many unordered pairs of different students have the same birthday? Do the same for unordered triplets of students. How to explain the discrepancy?

6. If each student independently selects a numeric PIN code of fixed length with uniform distribution, what is the minimal length (in digits) of the PIN code so that the probability of having two students selecting the same PIN code is lower than 1%?

[1] These numbers where the numbers in the Fall semester 2013.

Exercise 2 RSA for Paranoids

The purpose of this exercise is to study a variant of the RSA cryptosystem with a very large modulus which was proposed by Shamir.

1. Let us consider the regular RSA cryptosystem with $n = pq$ with p and q primes of s bits. What is the complexity of generating this key in terms of s?

Instead of taking p and q of same size, we take a prime p of s bits and a random number q (not necessarily prime, whose factorization is not necessarily known) of size ts (e.g., with $t \approx 10$) and we take $n = pq$ as in RSA. Assuming that messages m are integers of length less than s, i.e., $m \in \{0, 1, \ldots, 2^{s-1} - 1\}$, we encrypt m by computing $E(m) = m^e \bmod n$ like in RSA. The public key is the pair (n, e) as well.

2. What is the restriction on e in order to make E injective?
3. Under this restriction, explain how to decrypt.
4. What are the complexities of the encryption, the decryption, and the key generation?
5. When e is smaller than t, show that anyone can decrypt an intercepted ciphertext.
6. Show that finding the factor p of n is equivalent to the decryption problem.
7. Deduce that we can perform a chosen ciphertext attack (i.e., the adversary can access an oracle which outputs the plaintext of a given ciphertext) in order to recover the secret key.
8. How to thwart this attack?