Homework 7

1. **Safe Primes and Sophie Germain primes.** (20 points) In the lecture we raised the concern that it might be inefficient to generate a random element e in the set $\{0, 1, \ldots, \varphi(N) - 1\}$ that is relatively prime to $\varphi(N)$, where N is the product of two prime number p and q. In this problem we shall try to understand why picking p and q as *safe primes* helps.

   Recall the definition of safe primes. A prime $p = 2\alpha + 1$ is a *safe prime* if α is also a prime. The prime α is referred to as a *Sophie Germain prime*. For example, $7 = 2 \cdot 3 + 1$. So, $p = 7$ is a safe prime, and $\alpha = 3$ is a Sophie Germain prime.

   Suppose $p = 2\alpha + 1$ and $q = 2\beta + 1$ are distinct safe primes such that $\alpha, \beta > 2$. Note that $\varphi(N) = 4\alpha\beta$. We are interested in counting the number of elements in the set $\mathbb{Z}^*_{\varphi(N)}$. Equivalently, the number of elements in $\{0, 1, \ldots, \varphi(N) - 1\}$ that are relatively prime to $\varphi(N)$. This number is given by the following formula.

   $$4\alpha\beta \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{\alpha}\right) \left(1 - \frac{1}{\beta}\right)$$

   (You can use the principle of inclusion and exclusion to prove this result. For this problem, assume that this result is given to you.)

   If $p = 2\alpha + 1$ and $q = 2\beta + 1$ are distinct safe primes such that $\alpha, \beta > 2$, then prove that

   $$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{\alpha}\right) \left(1 - \frac{1}{\beta}\right) \geqslant \frac{4}{15}$$

   (Basically, this result shows that a number drawn uniformly at random from the set $\{0, 1, \ldots, \varphi(N) - 1\}$ is relatively prime to $\varphi(N)$ with probability at least $4/15$.)
   Solution.

2. **Number of Sophie Germain primes.** (10 points) It is conjectured that the number of Sophie Germain primes $< k$ is (roughly) equal to

$$\frac{Ck}{(\lg k)^2},$$

where C is a suitable positive constant. How many n-bit Sophie Germain primes are there?
Solution.

3. **Modification of RSA Encryption.** (20 points) Let p and q be distinct prime numbers and $N = p \cdot q$. In the class, to encrypt a message m, we appended a random string r to its prefix. We needed to ensure that the resulting number $(r\|m) \in \mathbb{Z}_N^*$. That is, we need $(r\|m)$ to be relatively prime to both p and q.

   In the class, we used the following trick. We ensured that $(r\|m)$ is smaller than both p and q. This technique ensures that $(r\|m)$ is relatively prime to both p and q. For example, if p and q are n-bit primes, then we were able to encrypt (roughly) $(n/2)$-bit message m using $(n/2)$-bit randomness r. In this problem we shall develop a more efficient encryption technique.

   Suppose $N \geqslant 2^{2t}$. Let the message $m \in \{0,1\}^{3t/2}$. Pick a random $r \xleftarrow{\$} \{0,1\}^{t/2}$. We want to argue that the probability of $(r\|m)$ being relatively prime to N is very high.

   Prove that, for any $m \in \{0,1\}^{3t/2}$, we have

$$\mathop{\mathbb{P}}_{r \xleftarrow{\$} \{0,1\}^{t/2}} \left[\gcd(r\|m, N) = 1\right] \geqslant 1 - \frac{2}{2^{t/2}}$$

   (This result shall allow using (roughly) $(3n/2)$-bit messages m with $(n/2)$-bit randomness r)
   Solution.

Collaborators :