Homework 1

1 Part I – Basic Number Theory

1. Compute $\varphi(n)$ for $n = 2, 5, 6, 8, 12$.

2. Compute:

    - $2^4 \mod 5$
    - $3^6 \mod 7$
    - $4^8 \mod 15$
    - $4^{24} \mod 15$
    - $15^{66} \mod 23$
    - $43^{48} \mod 105$

3. You should have noticed a pattern in the above computations. Try to generalize what is going on. Does the result of $33^{48} \mod 105$ contradict your conjecture? If no, congratulations. Otherwise, fix your generalization.

4. How many solutions does the equation $7x = 14 \mod 35$ have in $\mathbb{Z}_{35}$?

5. How many solutions does the equation $6x = 14 \mod 35$ have in $\mathbb{Z}_{35}$?

6. How many solutions does the equation $10x = 14 \mod 35$ have in $\mathbb{Z}_{35}$?

7. Try more examples and see if you can you generalize what is going on.

8. Find the multiplicative inverse of 22 in $\mathbb{Z}_{35}$.

9. Prove that if p is prime, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

10. Using the exercise above and the fact that $(a, b) = 1 \implies \varphi(ab) = \varphi(a)\varphi(b)$, prove the following formula for $\varphi(n)$ in terms of the factorization $n = \prod_{i=1}^{k} p_i^{\alpha_i}$:

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

11. Find an integer $n \in \mathbb{Z}^+$ such that

$$\frac{n}{\varphi(n)} > 10.$$

12. Write a program (say using the GMP library) that takes an integer ℓ as input and outputs a random prime number of ℓ bits. Use the output to plot the running time of GMP's `factor` program against the bit length of the inputs (where each input is the product of two equal length primes).

Bonus Number Theory Questions

NOTE: you might find the following a little more challenging. Don't kill yourself over these.

1. For any odd prime integer p, prove that $(p-1)! = -1 \mod p$.

2. Suppose that p is a prime, and that $p \equiv 3 \mod 4$. Show that there is no integer $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 = -1$. (Hint: think about Lagrange's theorem.)

3. Show that for any $c \in \mathbb{Z}^+$ there exists $n \in \mathbb{Z}^+$ such that $n/\varphi(n) > c$, *i.e.*, that $\limsup_{n\to\infty} n/\varphi(n) = \infty$.

2 Part II – Security Definitions

1. Let a M be a finite set of messages, and let $S(M)$ denote the set of all permutations of M (all bijective functions $f : M \to M$). We'll assume that if given a description of $\sigma \in S(M)$, both σ and σ^{-1} are efficiently computable. Suppose $P \subset S(M)$ is such that $\forall x, y \in M$, $\exists \sigma \in P$ such that $\sigma(x) = y$.

   (a) Show that $|P| \geq |M|$. (This is easy, but makes sure you've parsed the definition.)
   (b) Show that if $|P| = |M|$, then the following encryption scheme is *perfectly secure*, provided you only use it once:
   - Key generation: select a random $\sigma \in P$;
   - Encryption: $m \mapsto \sigma(m)$
   - Decryption: $c \mapsto \sigma^{-1}(c)$

   (c) Show that the above is false if $|M| < |P| < 2|M|$.
   (d) Observe that for any finite group G and any $g \in G$, the map $x \mapsto gx$ is a permutation of G. By viewing G itself as a set of permutations of G in this way, show that the above property is satisfied (with $M = P = G$).
   (e) The traditional `xor` one time pad is a special case of the above. What is the finite group in this case?

2. Suppose you want to encrypt a single bit, say via a OTP, but you only have access to a *biased* coin for key generation (that is, one outcome of the coin might be slightly more probable than the other). Show that if you use a single coin toss for key generation, your scheme will **not** be perfectly secure. How might you generate a uniformly random key (50/50 chance for 0/1) with this coin by flipping it multiple times? (This is a bit tricky!)

3. Suppose an encryption scheme acts on ascii-formatted plaintext messages by permuting the ascii characters. That is, a message $m = a_1 \ldots a_n$ would be encrypted as $a_{\pi(1)} \ldots a_{\pi(n)}$ for some (possibly randomized) permutation π (the a_i are the characters of the mesage). Prove such an encryption scheme can never be IND-CPA secure.

4. If an encryption scheme is IND-CPA secure, and if D is the decryption function, how must $|D^{-1}(x)|$ relate to the security parameter (asymptotically) for any (efficiently computable) x in the message space? Conclude in particular that a public-key, *deterministic* encryption scheme (like vanilla RSA) can never be IND-CPA secure.

5. Suppose a public-key cryptosystem encrypts integers (say, modulo another integer n). Let E, D denote the encryption and decryption algorithms, respectively. Show that if this scheme has the property that $D(E(x)E(y)) = x + y$ for any messages x, y, then the scheme is necessarily vulnerable to a CCA2 attack.

6. For IND-CPA security, recall that we had two definitions: a "game-style" definition, and the "semantic" definition, stating that for all distributions D on the message space M, and for all predicates $P : M \longrightarrow \{0, 1\}$, any efficient algorithm that predicts the predicate on input of a ciphertext will succeed with probability at most $l + \epsilon$, where

$$l = \max_{b \in \{0,1\}} \Pr_{m \xleftarrow{\$} D} [P(m) = b]$$

and where ϵ is negligible in the security parameter. Show that if an encryption scheme is secure according to the game-style definition, then it is secure under the semantic definition. *Note: the converse is also true. Try to prove that as well. It is a little harder though.*

7. Consider an encryption scheme (G, E, D) with the following property: in addition to the usual key generation algorithm G, there exists an algorithm $\widetilde{G}$ such that

   - $G(1^\lambda) \underset{\mathsf{PPT}}{\approx} \widetilde{G}(1^\lambda)$, and yet,
   - for $\widetilde{\mathsf{pk}} \leftarrow \widetilde{G}$, it holds that for all equal-length messages m_0, m_1, the distributions $E(\widetilde{\mathsf{pk}}, m_0), E(\widetilde{\mathsf{pk}}, m_1)$ are identically distributed.

   (a) Prove that any such cryptosystem must be IND-CPA secure.
   (b) Show how to construct such a cryptosystem based on the quadratic residuosity assumption (a simple modification of the Goldwasser-Micali cryptosystem suffices).