IV054 Coding, Cryptography and Cryptographic Protocols
2015 - Exercises VII.

1. Consider the following alternative way to decrypt an RSA cryptotext $c = m^e \mod n$. Assume that $p > q$.

   1. Calculate $d_p = d \mod (p-1)$.
   2. Calculate $d_q = d \mod (q-1)$.
   3. Calculate $q_{inv} = q^{-1} \mod p$.
   4. Calculate $m_p = c^{d_p} \mod p$.
   5. Calculate $m_q = c^{d_q} \mod q$.
   6. Calculate $h = q_{inv}(m_p - m_q) \mod p$.
   7. The decrypted message is $m = m_q + hq$.

   Show that this decryption procedure is correct, *ie.* $m_q + hq = c^d \mod n$.

2. A function f is *negligible* if and only if $\forall c \in \mathbb{N} : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : f(n) < n^{-c}$. A function f is *noticeable* if and only if $\exists c \in \mathbb{N} : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : f(n) \geq n^{-c}$. Prove or disprove the following:

   (a) A non-negligible function is not necessarily a noticeable function.
   (b) If both f and g are negligible, then $h(n) = f(n) + g(n)$ is also negligible.
   (c) If f is non-negligible and g is negligible, then $h(n) = f(n) - g(n)$ is non-negligible.

3. Let $h : \{0,1\}^m \to \{0,1\}^n$ be a strongly collision-free hash function. Let $h' : \{0,1\}^{2m} \to \{0,1\}^n$ be defined as
$$h'(x) = h(x_1) \oplus h(x_2),$$
   where x_1 is the first half of x and x_2 is the second half of x. Determine whether h' is strongly collision-free hash function.

4. Let f be a negligible function such that $f(n) \geq 0$ for all $n \in \mathbb{N}$. Let p be a polynomial such that $p(n) > 0$ for all $n \in \mathbb{N}$. Decide whether the following functions are negligible:

   (a) $f(n)p(n)$
   (b) $f(p(n))$

5. Consider the following cryptosystem:

   Key generation: Let k be an integer. Pick two different odd primes p and q of size $\frac{k}{2}$ bits, an element $e \in \mathbb{Z}_n$ such that $\gcd(e, \phi(n)) = 1$. Let $n = pq$ and $d = e^{-1} \bmod \phi(n)$.

   Public key: (e, n)

   Secret key: (d, n)

   Encryption: To encrypt a message $m \in \mathbb{Z}_n$, one picks a random $r \in \mathbb{Z}_n^*$ and computes the ciphertext $c = r^e(1 + mn) \bmod n^2$.

   Write the decryption algorithm and evaluate its complexity in terms of k.

6. Let p be an odd prime number.

   (a) Show that there exists a primitive root g modulo p such that $g^{p-1} \not\equiv 1 \pmod{p^2}$.
   (b) Conclude from (a) that g is a primitive root modulo p^2.

   (You may use without proof the fact that there exists a primitive root modulo p.)