Problem set 8

The problems marked [HPS] are from Hoffstein-Pipher-Silverman

(1) Let $p$ and $q$ be distinct primes, and let $e$ and $d$ be integers satisfying $de \equiv 1 \pmod{\ell}$ (where $\ell$ is the lcm $[p-1, q-1]$). Suppose further that $c$ is an integer with $\gcd(c, pq) > 1$. Prove that $x \equiv c^d \pmod{pq}$ is a solution to the congruence $x^e \equiv c \pmod{pq}$, thereby completing the proof of Theorem 1 of §III.D.

(2) Your RSA modulus is $n = 91$ and your encoding exponent is $e = 19$. Find the decryption exponent $d$. Why would $e = 9$ be a bad choice?

(3) The ciphertext 5859 was obtained using the RSA algorithm with public key $(n, e) = (11413, 7467)$. Find the original plaintext message (a number less than 11413) from which it was obtained. [Hint: factorize 11413 and then produce a decryption exponent.]

(4) Show that if $x^2 \equiv y^2 \pmod{n}$ and $x$ is not equivalent to $\pm y \pmod{n}$, then $(x + y, n)$ is a non-trivial factor of $n$.

(5) A decryption exponent for an RSA public key $(N, e)$ is an integer $d$ with the property that $a^d \equiv a \pmod{N}$ for all integers $a$ with $(a, N) = 1$.

Let $N = 38749709$. Eve’s magic box tells her that the encryption exponent $e = 10988423$ has decryption exponent $d = 16784693$ and that the encryption exponent $e = 25910155$ has decryption exponent $d = 11514115$. Use this information to factor $N$.

(6) Here is a cryptosystem which is supposed to be faster than RSA (and was apparently proposed at a cryptography conference): (1) Alice chooses two large primes $p$ and $q$ and publishes $N = pq$, then chooses 3 random numbers $g, r_1, r_2 \pmod{N}$ and computes $g_1 \equiv g^{r_1(p-1)} \pmod{N}$ and $g_2 \equiv g^{r_2(q-1)} \pmod{N}$. Her public key is the triple $(N, g_1, g_2)$ and her private key is $(p, q)$. (2) Bob wants to send the message $m \pmod{N}$ to Alice. He chooses two random numbers $s_1$ and $s_2 \pmod{N}$, computes $c_1 \equiv mg_1^{s_1} \pmod{N}$ and $c_2 \equiv mg_2^{s_2} \pmod{N}$, and sends the ciphertext $(c_1, c_2)$ to Alice. (3) Alice uses the CRT to solve the pair of congruences $x \equiv c_1 \pmod{p}$ and $x \equiv c_2 \pmod{q}$. (This part is faster than RSA for sure.)

(a) Prove that Alice’s solution $x$ is equal to Bob’s plaintext $m$.
(b) Explain why this cryptosystem is not secure. (Oops.)

(7) Formulate a man-in-the-middle attack, similar to the one we described for Diffie-Hellman, for the RSA cryptosystem.

(8) Use Pollard $p - 1$ method to factor $n = 48356747$.

(9) Suppose that the plaintext space $M$ of a certain cryptosystem is the set of bit strings of length $2k$. Let $e_k$ and $d_k$ be the encryption
and decryption functions associated with a key $k \in K$. This exercise describes one method of turning the original cryptosystem into a probabilistic cryptosystem.

Alice sends Bob an encrypted message by performing the following steps:

1. Alice chooses a $b$-bit message $m'$ to be encrypted.
2. Alice chooses a string $r$ consisting of $b$ random bits.
3. Alice sets $m = r \| (r \oplus m')$, where $\|$ denotes concatenation and $\oplus$ denotes XOR. Notice that $m$ has length $2b$ bits.
4. Alice computes $c = e_k(m)$ and sends the ciphertext $c$ to Bob.

(a) Explain how Bob decrypts Alice’s message and recovers the plaintext $m'$. (We assume that Bob knows the decryption function $d_k$.)
(b) If the plaintexts and the ciphertexts of the original cryptosystem have the same length, what is the message expansion ratio of the new probabilistic cryptosystem? (If a $b$-bit message gets converted to a $\mu b$-bit message, this ratio is $\mu$ by definition.)
(c) More generally, if the original cryptosystem has a message expansion ratio of $\mu$, what is the message expansion ratio of the new probabilistic cryptosystem?