MATH 75, HOMEWORK #6

EDGAR COSTA

(1) Recall that Alice signs a message m with her public key $(p, y) = (p, g^a)$, by picking a random number $e \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$, computing $r = g^e \pmod p$ and then finding $s \in \mathbb{Z}/(p-1)\mathbb{Z}$ such that

$$m = se + ar \pmod{p-1}.$$

One verifies the signature $(m, r, s) = (m, g^e, s)$ by checking

$$g^m = (y)^r r^s \pmod p.$$

(a) Show that by taking $r = g^e y \pmod{()p}$, where e is some random number in $\mathbb{Z}/(p-1)\mathbb{Z}$, and by picking an appropriate $s \in \mathbb{Z}/(p-1)\mathbb{Z}$ Eve can forge messages of the shape $m = es \pmod{p-1}$.

(b) One can prevent the previous attack by imposing a simple condition on the pair (r, s). Which one?

(c) Show that Even can circumvent such condition and still sign messages of the shape $m = es \pmod{p-1}$ by picking r and s in a different manner.

(d) Is this new forgery preventable? If so, how?

(2) Problem 2.28 (a) from the book.
Use the Pohlig–Hellman algorithm (Theorem 2.32) to solve the discrete logarithm problem

$$g^a = h \text{ in } \mathbb{F}_p$$

in each of the following cases.

(a) $p = 433$, $g = 7$, $h = 166$.

(3) Alice publishes her RSA public key: modulus $n = 2038667$ and exponent $e = 103$.

(a) Bob wants to send Alice the message $m = 892383$. What ciphertext does Bob send to Alice?

(b) Alice knows that her modulus factors into a product of two primes, one of which is $p = 1301$. Find a decryption exponent d for Alice.

(c) Alice receives the ciphertext $c = 317730$ from Bob. Decrypt the message.

(4) Alice uses the RSA public key modulus $n = pq = 172205490419$. Through espionage, Eve discovers that $(p\text{-}1)(q\text{-}1) = 172204660344$. Determine p, q.

(5) Bob uses RSA to receive a single ciphertext b corresponding to the message a. Suppose that Eve can trick Bob into decrypting a single chosen ciphertext c which is not equal to b. Show how Eve can recover a.

(6) Suppose that Alice and Bob have the same RSA modulus n and suppose that their encryption exponents e and f are relatively prime. Charles wants to send the message a to Alice and Bob, so he encrypts to get $b = a^e \pmod n$ and $c = a^f \pmod n$. Show how Eve can find a if she intercepts b and c.

Date: Due Thursday, 3 May 2018.

(7) A *Carmichael number* is an integer $n > 1$ that is *not* prime with the property that for all $a \in \mathbb{Z}$, $a^n \equiv a \pmod{n}$. Prove that $561, 1105, 1729$ are Carmichael numbers. *[Hint: Look at the proof of $a^{ed} \equiv a \pmod{n}$, $n = pq$, in RSA. You may factor these numbers!]*

(8) Bob chooses the RSA modulus

$$n = 1069524788729186444521284099154989216238375870617122680021373334588065126734368 7$$

and

$$e = 1857308780599082935579426134526996671022161384368318177549870987520554825439779$$

and because he is short for time chooses a small decryption exponent. Alice sends the secret message

$$b = 5876903442995476139711640244861982014547608694076473777226913452306949807294092$$

to Bob by converting her codeword of seven letters into ASCII bytes, interpreting this as the binary expansion of an integer, and encrypting it using RSA. Decrypt the message and recover the plaintext codeword.

(9) Let n be an RSA modulus, e_1 an encryption exponent, d_1 the corresponding decryption exponent, and e_2 a second encryption exponent. Given the data n, e_1, d_1, e_2, exhibit a fast and certain algorithm that determines the corresponding decryption exponent d_2 which does *not* use random choices, the factorization of n, or exponentiation modulo n. Illustrate your algorithm on $n = 119, e_1 = 23, d_1 = 23, e_2 = 7$ and $n = 119, e_1 = 23, d_1 = 23, e_2 = 11$.

(10) Problem 3.10 from the book.

Here is an example of a public key system that was proposed at a cryptography conference. It is supposed to be faster and more efficient than RSA.

Alice chooses two large primes p and q and she publishes $N = pq$. It is assumed that N is hard to factor. Alice also chooses three random numbers g, r_1, and r_2 modulo N and computes

$$g_1 \equiv g^{r_1(p-1)} \pmod{N} \qquad \text{and} \qquad g_2 \equiv g^{r_2(q-1)} \pmod{N}.$$

Her public key is the triple (N, g_1, g_2) and her private key is the pair of primes (p, q).

Now Bob wants to send the message m to Alice, where m is a number modulo N. He chooses two random integers s_1 and s_2 modulo N and computes

$$c_1 \equiv m{g_1}^{s_1} \pmod{N} \qquad \text{and} \qquad c_2 \equiv m{g_2}^{s_2} \pmod{N}.$$

Bob send the ciphertext (c_1, c_2) to Alice.

Decryption is extremely fast and easy. Alice uses the Chinese remainder theorem to solve the pair of congruences

$$x \equiv c_1 \pmod{p} \qquad \text{and} \qquad x \equiv c_2 \pmod{q}.$$

(a) Prove that Alice's solution x is equal to Bob's plaintext m.

(b) Explain why this cryptosystem is not secure.