Math 412 Adventure Sheet on RSA

ENCRYPTION PROBLEM 1: Suppose I want you to send me a message by a messenger pigeon, but I want to make sure that nobody who intercepts messenger pigeons is able to understand the message. To do this, I want to send you a pigeon with instructions on how to encrypt your message. If this is going to work, we want to ensure that

($\star$) knowledge of the encryption rule does not give away the decryption rule.

Furthermore, if we want lots of people to be able to send lots of different messages, we would like a source of lots of similar but distinct encryption rules, each of which comes with an easy-to-use decryption rule. For the first two encryption rules, we will assume our message is a number.

A. FAKE RSA: A BAD ENCRYPTION RULE. Let p be a prime number.

(1) Show that if $p \nmid a$ and $(p-1)|c$, then $a^c \equiv 1 \mod p$.
(2) Show that for any integer a, if $c \equiv 1 \mod p-1$, then $a^c \equiv a \mod p$.
(3) Let e be an integer with $(e, p-1) = 1$. Explain why there exists a solution d to the equation $ed \equiv 1 \mod p-1$.
(4) Consider the following encryption rule: for each message a, where $0 \leqslant a \leqslant p-1$, we encrypt the message via $E(a) = [a^e]_p$. Show that $D(b) = [b^d]_p$, with d as in the previous part, is the corresponding decryption rule.
(5) To use this encryption rule in the context of the above storyline, I need to send you the integers p and e (or the function E). Explain how a pigeon interceptor would know how to find d (and the function D).
(6) Suppose that you intercept a message that you know is encoded by this algorithm, and you previously intercepted the encryption parameters $p = 107$ and $e = 13$. Find the decryption function.

Solution.

(1) The group $\mathbb{Z}_p^\times$ has $p-1$ elements, so every element has order dividing $p-1$. In particular, $[a]_p^{p-1}$ is the identity of $\mathbb{Z}_p^\times$, which is 1. Thus, if c is a multiple of $p-1$, $[a]_p^c = [1]_p$, so $a^c \equiv 1 \mod p$.
(2) If $p \nmid a$, then by the previous part $a^{c-1} \equiv 1 \mod p$, so $a^c \equiv a \mod p$. If $p \mid a$, then $[a]_p = [0]_p$, so $[a]_p^t = [0]_p = [a]_p$ for any t.
(3) If $(e, p-1) = 1$, then e is a unit in $\mathbb{Z}_{p-1}$, so there is a $d \in \mathbb{Z}$ such that $[d]_{p-1} \in \mathbb{Z}_{p-1}$ satisfies $[e]_{p-1}[d]_{p-1} = [1]_{p-1}$. That is, $ed \equiv 1 \mod p-1$.
(4) $D(E(a)) = [(a^e)^d]_p = [a^{ed}]_p$. Since $ed \equiv 1 \mod p-1$, by part (2), $[a^{ed}]_p = [a]_p$ for all a.
(5) Given p and e with $(p-1, e) = 1$ we (or anyone with similar traning) can solve for a d such that $ed \equiv 1 \mod p-1$, and thus find a decryption rule.
(6) We use the Euclidean algorithm to find an inverse for 13 mod 106: 49 works. the decryption function is $D(b) = [b^{49}]_{107}$.

B. RSA: A GOOD ENCRYPTION RULE. Let p and q be two prime numbers, and let $n = pq$.

(1) Consider the map $\psi : \mathbb{Z} \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q$ given by $\psi(a) = ([a]_p, [a]_q)$.

(a) Check that this is a ring isomorphism.
(b) Show that $\mathbb{Z}_n^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$.

(2) Let $k = (p-1)(q-1)$. Show that if $c \equiv 1 \mod k$, then $c \equiv 1 \mod p-1$ and $c \equiv 1 \mod q-1$.
(3) Show that if $c \equiv 1 \mod k$, then $a^c \equiv a \mod n$.
(4) Let e be an integer with $(e, k-1) = 1$. Explain why there exists a solution d to the equation $ed \equiv 1 \mod k$.
(5) Consider the following encryption rule: for each message a, where $0 \leqslant a \leqslant n-1$, we encrypt the message via $E(a) = [a^e]_n$. Show that $D(b) = [b^d]_n$ is the corresponding decryption rule.
(6) To use this encryption rule in the context of the above storyline, I need to send you the integers n and e (or the function E). Explain why a pigeon interceptor would now have much more trouble finding d (and the function D).
(7) What other piece of information would a pigeon interceptor want to know in order to find d?
(8) Use the encryption rule corresponding to the numbers $n = 221$ and $e = 7$ to encrypt the message $a = 42$. Now find the corresponding decryption rule and check that you get your message back. In other words, break RSA!
(9) One could also try to find a way to use encryption to ensure that the sender is who they claim they are. Suppose that Jack and Eloísa know each other's encryption information $(n_{\text{jack}}, e_{\text{jack}})$ and $(n_{\text{eloísa}}, e_{\text{eloísa}})$; these are also called public keys. How could they send encoded messages in such a way to ensure that they know they are the senders?[1]

Solution.

(1) We have done this already!
(2) This is clear.
(3) In this case, by part (2), $c \equiv 1 \mod p-1$ and $c \equiv 1 \mod q-1$. Thus, $a^c \equiv a \mod p$ and $a^c \equiv a \mod q$, by A(2). Thus, $p|(a^c - a)$ and $q|(a^c - a)$, so $n|(a^c - a)$.
(4) Same as A(3).
(5) Same as A(4), using B(3).
(6) To find D (equivalently d) we would want to know k. It is easy to find k if we know p and q, but we were only told n. We would need to factor it (or something similar) to find k.
(7) k, or p and q.
(8) $E(42) = [42]_{221}^7 = [185]_{221}$. To find the decryption rule, we factor $n = 13 \times 17$, and find $k = 12 \times 16 = 192$. We now need the inverse of $[7]_{192}$ in $\mathbb{Z}_{192}$. We can use the Euclidean algorithm to find $[55]_{192}$ as an inverse. This means that the decryption rule is $D(x) = [x]_{221}^{55}$. Now, $[185]_{221}^{55} = [42]_{221}$.
(9) Jack can send the function $E_{\text{ELOÍSA}} \circ D_{\text{JACK}}$ to codify his messages. Recall that everybody knows the function E_{JACK}, but only Jack knows D_{JACK}. If Eloísa knows that he plans on doing this, she can decode his messages, without knowing the decoding function D_{JACK}: she can decode via the function $E_{\text{JACK}} \circ D_{\text{ELOÍSA}}$. If she ends up with something that makes sense at the end (or maybe has a predetermined passphrase) then she knows that the person who sent the message knows the decryption function corresponding to (n, e)!

ENCRYPTION PROBLEM. Suppose I want you to send me a message by a messenger pigeon (or smoke signals), but I want to make sure that nobody who intercepts messenger pigeons to be able to understand the message. To do this, I want to create a secret password by exchanging messages, and then use the

[1] Hint: can the roles of decryption and encryption be swapped somehow? Also, it may be useful to compose two functions here.

password to lock up the message in such a way that only someone with the password can unlock it. Let's not worry here about how to lock up messages with a password, but just worry about creating a secret password. If this is going to work, we might each choose secret starting data, but

$\star$ knowledge of any shared data does not give away the password.

Furthermore, if we want lots of people to be able to send lots of different messages, we would like a source of lots of similar but distinct passwords.

C. DIFFIE-HELLMAN KEY EXCHANGE. Let p be a prime number.

(1) Explain why there exists a number x such that for every n with $p \nmid n$, we can write $n = x^m \mod p$ for some integer m.
(2) If $A = [x^a]_p$ and $B = [x^b]_p$, then why is $A^b = B^a$?
(3) Say I (secretly) choose an integer a and you (secretly) choose an integer b, and then I send you A and you send me B. How can we agree on a password?
(4) To use this password rule in the context of the above storyline, we need to send the integers p and x, and the classes A and B. How would a pigeon interceptor find the password? What other information would a pigeon interceptor want to know?
(5) In your group, choose two people to create a password, and other people to be password hackers. Follow the recipe above (with a two digit prime) to create a password; the password hackers' goal is to guess the password. After doing this, switch roles. How secure do you think this key exchange is? What if the prime is larger?

Solution.

(1) The multiplicative group of a finite field is cyclic!
(2) Both sides are $[x^{ab}]_p$.
(3) I take B^a and you take A^b; they are the same!
(4) A pigeon interceptor would need to find a or b. In general, it turns out to be relatively difficult to solve $A = x^a$ for a in a finite field.