Ilana Sivan
205634272
Honors Course
Homework 5

Question 1

We will assume that instead of using modulo N (which is a product of two primes encryted by RSA), modulo of a prime p. As in RSA, we would have a public key (p, e), and the encryption of a message $m \bmod p$ would be $m^e \bmod p$. Prove that this system is not secure, by giving an efficient algorithm to decrypt: that is, show an algorithm that given $p, e, m^e \bmod p$ as input, outputs $m \bmod p$. Justify the correctness and analyze the running time of your algorithm.

We will first assign $\mathrm{m^e modp}$ to some variable, s for the purpose of simplifying our algorithm. Our algorithm will efficiently output $m \bmod p$ thereby recovering the message. We will construct an algorithm that will use the Eucledian algorithm and return a modular exponentiation. We choose an encryption exponent e in RSA, such that $\mathrm{gcd(e, p-1) = 1}$, so e is relatively prime to $\mathrm{p-1}$, and we have an inverse mod of $\mathrm{p-1}$. So we get that $\mathrm{de = k(p-1)+1}$ for some $\mathrm{k} \in \mathbb{Z}$.

Now we can compute and get that $\mathrm{s^d \equiv m^{ed} = m^{k(p-1)+1} = (m^{p-1})^k * m} \equiv m \bmod p$

Therefore, our algorithm looks like so:

```
Decrypt(p,e,s):

    d ← ExtendedEuclid(e, p-1)
    return ModExp(c,d,p)
```

The runtime of our algorithm is $\mathrm{O(n^3)}$ where n is the length of the binary representation of p.

Question 2

Prove that if $\mathrm{N} = \mathrm{pq}$ can be factored efficiently, then the RSA system is unsafe. Hint: use the previous question and the Chinese Remainder Theorem.

We will assume that we can indeed factor efficiently, and we recall that in RSA that the recipient knows (e, N), so we factor $\mathrm{N} = \mathrm{pq}$ where p,q are unique values and prime, thereby RSA indeed holds.

For some message m which is sent to the recipient, we use our previous algorithm and call:

`Decrypt`$(e, (p - \mathit{1})(q - \mathit{1}), m)$ and we can get $e^{-\mathit{1}} = d$, thereby decrypting our message and leaving the system unsafe.

Question 3

In an RSA system the public key (N, e) is known to everyone. Suppose that the private key d is compromised. Show that if $e = 3$ then you can efficiently factor $N = pq$.

In an RSA system, the primes p and q in $N = pq$ are generated to be the same length, so as they are of the same length they are of the order $\sqrt{N}$, so we have $\frac{p+q-1}{N}$ which approaches 0 for large N. We know that in an RSA system we have $\mathrm{ed} \equiv 1(\mathrm{mod}\varphi(\mathrm{N}))$, so we know that there exists a congruence for some $\mathrm{k} \in \mathbb{Z}$, such that $\mathrm{ed} - 1 = \mathrm{k}\varphi(\mathrm{N})$. If we replace our $\varphi(N)$ with$(\mathrm{p}-1)(\mathrm{q}-1)$ we get the following:

$\mathrm{ed} - 1 = \mathrm{k}(\mathrm{p}-1)(\mathrm{q}-1)$
$\mathrm{ed} - 1 = \mathrm{k}(\mathrm{pq}-\mathrm{p}-\mathrm{q}+1)$
$\mathrm{ed} - 1 = \mathrm{kN} - \mathrm{k}(\mathrm{p}+\mathrm{q}-1)$
$\frac{\mathrm{ed}-1}{\mathrm{N}} = \mathrm{k}(1 - \frac{\mathrm{p}+\mathrm{q}-1}{\mathrm{N}})$

So here we can assume k to be the nearest integer to $\frac{ed-1}{N}$. With a compromised d, we can calculate k, and with this k we can calculate $p + q$ with $\mathrm{N} - \frac{\mathrm{ed}-1}{\mathrm{k}} + 1$. As we know that $N = pq$ we solve the following system:

$\mathrm{pq} = \mathrm{N}$
$\mathrm{p} + \mathrm{q} = \mathrm{N} - \frac{\mathrm{ed}-1}{\mathrm{k}} + 1$

We know then that $\mathrm{de} = 3\mathrm{d} = 1(\mathrm{mod}(\mathrm{p}-1)(\mathrm{q}-1))$, so $3\mathrm{d} - 1 = \mathrm{k}(\mathrm{p}-1)(\mathrm{q}-1)$. Therefore, $\frac{3d-1}{k} = (p-1)(q-1)$.

As we know that $(\mathrm{p}-1)(\mathrm{q}-1) < \mathrm{N}$, we have the following equivalence: $\frac{3d-1}{k} < N$. Given that $d = e^{-1} mod (p-1)(q-1) < N$, we have $3\mathrm{d} - 1 < 3\mathrm{N}$, so $1 \leq \mathrm{k} \leq 3$. We compute:

$\frac{3d-1}{k(p-1)} = q - 1$
$\frac{3d-1}{k(p-1)} + 1 = q$
$\mathrm{N} = \mathrm{pq} = \mathrm{p}(\frac{3\mathrm{d}-1}{\mathrm{k}(\mathrm{p}-1)} + 1)$
As above :)

We can see that we have now factored $\mathrm{N} = \mathrm{pq}$

Question 4

Alice and her three friends are RSA users. Alice's three friends have public keys $(N_1, 3)$,$(N_2, 3)$, $(N_3, 3)$ respectively (that is to say that in all three cases $e = 3$, and $N_i = p_i q_i$ for n-bit primes $\mathrm{p_i}, \mathrm{q_i}$). Show that if Alice sends the same message m encrypted with RSA, then anyone who intercepts all three encrypted messages will be able to efficiently find m. (Hint: use the Chinese Remainder Theorem)

Alice is sending the same message m to all of her friends, and the public keys are in the form (N_i, e_i) where $\mathrm{i} = 3$. So we have $m^3 \mathrm{mod} N_1$, $m^3 \mathrm{mod} N_2$, $m^3 \mathrm{mod} N_3$. We can then observe the group $\mathbb{Z}_{N_1 N_2 N_3}$, the multiplicative group for modulo inverses of $\mathrm{N_1}, \mathrm{N_2}, \mathrm{N_3}$, as we did in previous units: $\mathbb{Z}_{N_1 N_2 N_3} = \{0, ..., N_1 N_2 N_3 - 1\}$.

Then we can suppose that for any $1 \leq \mathrm{a},\ \mathrm{b} \leq 3$ there is $\mathrm{gcd}(\mathrm{N_a}, \mathrm{N_b}) = 1$ such that they are coprime, and we assume that we do not select the same values for a and b in the initialization of our key, so $\mathrm{a} \neq \mathrm{b}$.

We know from the remainder theorem that there exists a **single** $\mathrm{x} \in \mathbb{Z}_{N_1 N_2 N_3}$ such that $\mathrm{x} = m^3 \mathrm{mod} N_\mathrm{y}$, $1 \leq \mathrm{y} \leq 3$. So we get $\mathrm{m} = (\mathrm{m}^3)^{\frac{1}{3}} \mathrm{mod} \mathrm{N_1 N_2 N_3}$