Security of RSA and El-Gamal

Exercice 1. Common modulus attack

Bob was issued a very strong (16384 bits) RSA key (n, e) and uses it to encrypt a file with the list of all of his password, using text-book RSA (without padding). Later on, as he is a bit paranoid, he decides to change his key. However he no longer has access to a powerfull computer that can generate a new pair of primes of the same size. He therefore decides to keep the same modulus but change his public and private exponents. His new public key is now (n, f) where e and f are coprime.

a. Eve has intercepted the two versions of the encrypted password file. Explain how she can now recover the plaintext of the password file.

Exercice 2. IND-CPA vulnerability

a. Explain what game defines the IND-CPA security

b. Apply it to text-book RSA to show that it is not IND-CPA secure

Exercice 3. OW-CCA vulnerabilities

a. Explain what game defines the OW-CCA security

b. Propose an attack showing that textbook RSA is not OW-CCA secure.

c. Same question for El-Gamal cryptosystem.

d. Is this weakness related to the fact that the cryptosystem is deterministic ?

Exercice 4. Broadcast attack

We again consider textbook RSA. Suppose Alice sends the same message m to three recipients : Bob with public key $(n_B, 3)$, Chris with public key $(n_C, 3)$ and Dan with public key $(n_C, 3)$. Having a fixed public exponent equals to three has been standard for a long period of time.

a. Explain how Eve who intercepts the three corresponding ciphertexts can recover the plaintext without using any private key.

Exercice 5. Factorial attack

Let $B \in \mathbb{Z}$ such that $(p-1)$ divides $B!$.

a. Show that for any prime factor p_1 of $p-1$, $p_1 \leq B$.

b. For $a \in \mathbb{Z}$ show that $a^{B!} = 1 \mod p$.

c. Let $A = a^{B!} \mod n$. Show that p divides $A - 1$.

d. How much does the computation of A costs (as a function of n and B)

e. How can one try to factor n using the above results ? Under which condition does it work ?

f. Contermeasure ?

Exercice 6. RSA decryption variant

Let's consider the following variant on RSA : for $n = pq$ with p and q prime numbers
— let $\mu(n) = \frac{(p-1)(q-1)}{\delta}$ where $\delta = \gcd(p-1, q-1)$.
— The public key is still a pair (e, n) where e is co-prime with $(p-1)(q-1)$
— let $d' = e^{-1} \mod \mu(n)$ so that the private key now becomes (d', n)
— encryption is $E(x) = x^e \mod n$
— decryption is $D(x) = x^{d'} \mod n$

a. Explain why the decryption still works

b. compute the private keys d and d' for $p = 19$ and $q = 31$ and $e = 7$.

c. What do you think of this variant in terms of efficiency and security ?