ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ & ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
SCHOOL OF INFORMATION SCIENCES & TECHNOLOGY
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
DEPARTMENT OF INFORMATICS

Ειδικά Θέματα Αλγορίθμων
Ασκήσεις Φροντιστηρίου #4
RSA

1. The ciphertext 5859 was obtained from the RSA algorithm using $n = 11413$ and $e = 7467$. Using the factorization $11413 = 101 \cdot 113$, find the plaintext.

2. Let n be the product of two large primes. Alice wants to send a message m to Bob, where $gcd(m, n) = 1$. Alice and Bob choose integers a and b, which are relatively primes to $\phi(n)$. Alice computes $c = m^a (\mod n)$ and sends c to Bob. Bob computes $d = c^b (\mod n)$ and sends d back to Alice. Since Alice knows a, she finds a_1 such that $aa_1 = 1(\mod \phi(n))$. Then she computes $e = d^{a_1} (\mod n)$ and sends e to Bob. Explain what Bob must now do to obtain m, and show that this works.

3. Naive Nelson uses RSA to receive a single ciphertext c, corresponding to the message m. His public modulus is n and his public encryption exponent is e. Since he feels guilty that his system was used only once, he agrees to decrypt any ciphertext that someone sends him, as long as it is not c, and return the answer to that person. Eve sends him the ciphertext $2^e c(\mod n)$. Show how this allows Eve to find m.

4. Suppose two users Alice and Bob have the same RSA modulus n and suppose that their encryption exponents e^A and e^B are relatively prime. Charles wants to send the message m to Alice and Bob, so he encrypts to get $c_A = m^{e_A} (\mod n)$ and $c_B = m^{e_B} (\mod n)$. Show how Eve can find m if she intercepts c_A and c_B.

5. Suppose Alice uses the RSA method as follows. She starts with a message consisting of several letters, and assigns $a = 1, b = 2, ..., z = 26$. She then encrypts each letter separately. For example, if her message is cat, she calculates $3^e (\mod n)$, $1^e (\mod n)$ and $20^e (\mod n)$. Then she sends the encrypted message to Bob. Explain how Eve can find the message without factoring n. In particular, suppose $n = 8881$ and $e = 13$. Eve intercepts the message:

$$4461\ 794\ 2015\ 2015\ 3603.$$

Find the message without factoring 8881.

6. Let $n = p \cdot q$ be the product of two distinct primes.
a) Let m be a multiple of $\phi(n)$. Show that if $gcd(a, n) = 1$, then $a^m = 1(\mod p)$ and $(\mod q)$.
b)Let m be a multiple of $\phi(n)$ and let a be arbitrary (possibly $gcd(a, n) \neq 1$). Show that $a^{m+1} \equiv a(\mod p)$ and $(\mod q)$.
c)Let e and d be encryption and decryption exponents for RSA with modulus n. Show that $a^{e \cdot d} \equiv a(\mod n)$ for all a. This shows that we do not need to assume $gcd(a, n) = 1$ in order to use RSA.
d) If p and q are large, why is it likely that $gcd(a, n) = 1$ for a randomly chosen a?