ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

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

ΕΙΔΙΚΑ ΘΕΜΑΤΑ ΑΛΓΟΡΙΘΜΩΝ

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.

Hint: Calculate $\phi(n) = (p-1)(q-1)$ using the provided prime factors $p = 101$ and $q = 113$. Use the Extended Euclidean Algorithm to find the private key d such that $de \equiv 1 \pmod{\phi(n)}$. Retrieve the plaintext by computing $m \equiv c^d \pmod{n}$.

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 $c = m^a \pmod{n}$ and sends c to Bob. Bob computes $d = c^b \pmod{n}$ and sends d back to Alice. Since Alice knows a, she finds a_1 such that $aa_1 = 1 \pmod{\phi(n)}$. Then she computes $e = d^{a_1} \pmod{n}$ and sends e to Bob. Explain what Bob must now do to obtain m, and show that this works.

Hint: First, Double Encryption: Alice encrypts the message m with her exponent a ($c \equiv m^a$), and Bob applies his own encryption exponent b on top of it ($d \equiv c^b \equiv m^{ab} \pmod{n}$). Next, Alice Removes Her Key: Alice calculates the modular inverse a_1 such that $a \cdot a_1 \equiv 1 \pmod{\phi(n)}$. She applies this to the message d, effectively cancelling out her original exponent a to produce $e \equiv d^{a_1} \equiv m^b \pmod{n}$. Finally, Bob Removes His Key: Bob calculates the inverse b_1 of his exponent ($b \cdot b_1 \equiv 1$). He decrypts the final message e to recover the original text: $e^{b_1} \equiv (m^b)^{b_1} \equiv m \pmod{n}$, which holds true by the Corollary of Euler's Theorem.

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 $2^e c \pmod{n}$. Show how this allows Eve to find m.

Hint: Eve sends Nelson $2^e c \pmod{n}$. Nelson returns $m_1 \equiv (2^e c)^d \equiv 2^{ed} \cdot c^d \equiv 2m \pmod{n}$ because $ed \equiv 1 \pmod{\phi(n)}$. Eve recovers the original message m by simply multiplying Nelson's result by $2^{-1} \pmod{n}$.

4. 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 $a^m = 1 \pmod{p}$ and $\pmod{q}$.
b)Let m be a multiple of $\phi(n)$ and let a be arbitrary (possibly $gcd(a, n) \neq 1$). Show that $a^{m+1} \equiv a \pmod{p}$ and $\pmod{q}$.
c)Let e and d be encryption and decryption exponents for RSA with modulus n. Show that $a^{e \cdot d} \equiv a \pmod{n}$ 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?

Hint: (a): First, since m is a multiple of $\phi(n)$, write $m = k \cdot \phi(n)$. By Euler's Theorem, we know that if $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$. Raising both sides to the power of k yields $a^m \equiv 1^k \equiv 1 \pmod{n}$, which implies the relation holds modulo the factors p and q.
(b): To prove $a^{m+1} \equiv a \pmod{p}$ for any integer a: Case 1 ($p \nmid a$): By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. Since m is a multiple of $\phi(n) = (p-1)(q-1)$, m is also a multiple of $p-1$. Thus, $a^{m+1} = a \cdot (a^{p-1})^c \equiv a \cdot 1 \equiv a \pmod{p}$. Case 2 ($p \mid a$): If a is a multiple of p, then $a \equiv 0 \pmod{p}$. The equation becomes $0^{m+1} \equiv 0$, which is trivially true. Since this holds for both prime factors p and q, it holds for their product n.
(c) First, recall the key property of RSA exponents: $e \cdot d \equiv 1 \pmod{\phi(n)}$, which implies $e \cdot d - 1$ is a multiple of $\phi(n)$. Let $m = e \cdot d - 1$. Next, apply the result from Part (b) (proved in the previous exercise), which states that for any m divisible by $\phi(n)$, $a^{m+1} \equiv a \pmod{n}$ holds for all integers a (even those sharing factors with n). Finally, substitute our specific exponent back in: $a^{e \cdot d} = a^{m+1} \equiv a \pmod{n}$, proving that RSA decryption works for every possible message.
(d) First, the probability that a random number $a < n$ is coprime to n is exactly the ratio $\frac{\phi(n)}{n}$. Next, expand this using the formula $\phi(n) = (p-1)(q-1)$:

$$P(\gcd(a, n) = 1) = \frac{(p-1)(q-1)}{pq} = \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)$$

Finally, observe that as p and q grow very large ($p, q \to \infty$), the fractions $\frac{1}{p}$ and $\frac{1}{q}$ approach 0. Thus, the total probability approaches 1, meaning it is statistically almost certain that a randomly chosen message will be coprime to n.