Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 10
Version 02.07.2020

Exercise 1.

Let $p := 3$, $q := 11$, as well as $n := pq$ and consider the associated RSA algorithm with encryption coefficient $e := 17$. Noting that $0, 1, 32 \in \mathbb{Z}_{33}$ are fixed points of the associated RSA algorithm, we investigate the following plain text alphabet $\mathcal{A} := \{z_i \,|\, i \in \{2, \ldots, 31\}\}$ for encryption via the RSA:

i	z_i	i	z_i	i	z_i	i	z_i	i	z_i	i	z_i
2	A	7	F	12	K	17	P	22	U	27	Z
3	B	8	G	13	L	18	Q	23	V	28	
4	C	9	H	14	M	19	R	24	W	29	!
5	D	10	I	15	N	20	S	25	X	30	?
6	E	11	J	16	O	21	T	26	Y	31	.

a) Encrypt the plaintext `TAU CETI` using the RSA algorithm.

b) Decrypt the cipher text `YIZXG?` which has been created using the above RSA algorithm.

Exercise 2.

For distinct odd primes $p, q \in \mathbb{P}$, let $n := pq$ be the associated RSA module. Show that one can easily find p and q only from the knowledge of n and $\varphi(n)$ by solving a certain quadratic equation.
Hint: Observe that precisely p and q are the roots of the polynomial:
$x \mapsto (x - p)(x - q)$. Rearrange the latter.

Exercise 3.

Let $n = p \cdot q$ be the product of two different unknown prime numbers. Let e, d be two integers such that $e \cdot d = 1 \; mod \; \varphi(n)$.

a) Show that $x^2 \equiv 1 \mod n$ has exactly four solutions in $\mathbb{Z}_n$.

b) Why the $gcd(x - 1, n)$ is equal to p or q, where x is nontrivial solution of the equation in a)?

c) Show that $a^k \equiv 1 \mod n$ for every $a \in \mathbb{Z}_n$, where $k := e \cdot d - 1$.

d) Why exist $r, t \in \mathbb{N}$ such that $k = 2^t \cdot r$ with r odd and $t \geq 1$?

e) Show that one element of the sequence $a^{\frac{k}{2^i}} \mod n$, $i = 1, ..., t$ is a solution of the equation in a).

f) How can you factor n given encryption and decryption coefficient e and d?