PCC – PAK-CRYPT CHALLENGE

Rules & Regulations of Pak-Crypt Challenge 2022

This challenge consists of two rounds scheduled over 4 days.

Round 1 (Qualifier) – 3 days 22nd – 24th July

Round 1, which can also be referred to as the ***Qualifier*** has the set of rules as follows:-

1. It will consist of 3 days (22 – 24th July), with a 2-hour long activity each day, online (3:00 pm – 5:05pm; extra 5 minutes are to upload the solutions).
2. The aim of round 1 is to check the cryptographic aptitude of participants.
3. Every candidate will participate individually in this round.
4. During the activity hours, the use of Internet is allowed. Camera and mic must be on.
5. However, discussion with other participants or call to a friend is not allowed and will result in disqualification from the competition. So you all need to be very careful as you will be actively monitored.

6. Please note that Round 1 will act as the filtration stage for candidates participating in Round 2. Participants that qualify for Round 2 will be awarded with a certificate of qualification.
7. The result of Round 1 will be announced on 25th July, Monday.
   (Note: The decision of jury will stand final, with no amendments or revisions expected)

Round 2 (Finale) – 1 day 27th July

After the results, the participants that qualify Round 1 will proceed towards Round 2 and compete each other on 27th of July.

1. Round 2 will consist of a 4-hour (1pm – 5pm) long activity, on-site at NCCS Air University, Islamabad.
2. Bring your own laptop with programming languages tools/platforms installed (MATLAB, Programming Language of your choice, etc.) WiFi access shall be provided.
3. It is a team Challenge, so each of you will become part of a team comprising of 3 individuals. Please note that, according to your affiliations, teams will be made by advisory committee and will be announced on 27th July. Just keep in mind, that at least one member of your team must have a good background of cryptographic domain.
4. Round 2 result will be announced on 28th July (3:30 pm – 4:30 pm).
5. The most exciting part:-
   a. Winning team will be awarded a cash prize of 6 lacs.

b. 3 runner-up teams will be awarded cash prize of 2 lacs each.

c. Chances for mentorship for future national/international events.

Sample Question for preparation:

Sample Question for Round 1

Q # 1:- An Encryption scheme is defined as follows;

i. The key is normally a permutation of the 26 English letters e.g. “sexrctadfhjnvwopuibygzqlkm” and “nrgxvdpuymascowzhklbeiqftj” are two possible permutations.

ii. Another part of the key is a pair of numbers with value between 0 and 9. e.g. (3,9) or (0,5) etc.

iii. The third and final part of the key is a number of any length e.g. 89654321 or 632

iv. The cipher scheme is setup with in the following way for permutation “quztelkjfwcvgbdahpisrnoxmy” and number pair (3,6)

	0	1	2	3	4	5	6	7	8	9
	q	u	z		t	e		l	k	j
3	f	w	c	v	g	b	d	a	h	p
6	i	s	r	n	o	x	m	y		

Table 1

- Note that in the first row, there is a gap for the column numbers 3 and 6.
- The second and third rows are marked with the key pair numbers i.e. 3 and 6.
- There are 30 possible values for 28 possible spots (excluding the two key pair columns) so it is also possible to introduce space of a maximum of two slots in rows 2 and 3. E.g. we can change the above scheme to

	0	1	2	3	4	5	6	7	8	9
	q	u	z		t	e		l	k	j
3	f	w	c	v	g	b	d	a		h
6	p	i	s	r		n	o	x	m	y

Table 2

- But it is important that both parties know about this change as well.

v. For the encryption process, in the first stage, the alphabets of plaintext appearing in 1st row are simply replaced by the column numbers and the alphabets appearing in 2nd or 3rd row are replaced by the row and then the column number e.g. the plaintext "idonotcareaboutu" is encrypted using system of TABLE1 as "60366463644323762537356414 1"

vi. In the second stage, the ciphertext from stage 1 is added to the third part of the key e.g. 6390 using non-carrying addition
It becomes

```
  60366463644323762537356414 1
+ 63906390639063906390639063 9
  23262753273386668827985477 0
```

Converting it back to alphabets using Table1, we will get "zcrleclvkm ljketllq"

Question: - Suppose the used keys are "dcbiatrzmjglnxvyspfeokqhuw", (6,7), and 893 and we receive the ciphertext "czdddunbcddpip", What was the plaintext?

Solution:
Keys are "dcbiatrzmjglnxvyspfeokqhuvw, (6,7)"
For addition: 893
Cipher text is "czdddunbcddpip"
Plaintext =???

In order to get plaintext, start the encryption procedure in reverse order.
First make the table like table 1 by using the given keys then convert the Ciphertext into numbers by using that table. At the end, subtract that numbers from the key 893 instead of addition.

	0	1	2	3	4	5	6	7	8	9
	d	c	b	i	a	t			r	z
6	m	j	g	l	n	x	v	y	s	p
7	f	e	o	k	q	h	u	w		

Cipher text becomes
190007664210069369
Now, subtraction

```
  190007664210069369
- 893893893893893893
  307214871427276576
```

So, plaintext is “I do care about U”

Sample Question for Round 2

Suppose we were using RSA for secure communication using the public value ‘n”. But somehow the value of ϕ(n) gets disclosed to the user. Show that RSA has been broken now by providing the values of prime numbers p and q for the following values.
n= 100000000010000000002379
ϕ(n) = 100000000009800000002280

Submission Guidelines:

Answers are to be submitted by scanning your solution on paper/digital document. You will be asked to submit your answers on google forms against each question.