PakCrypt

International Symposium

2025

PakCrypt.Org

PakCrypt

International Symposium

2025

PakCrypt.Org

Important Dates	
Pre-Qualifier Round for PakCrypt Cryptography Competition	01-Aug-2025 to 30-Sep-2025
Qualifier Round PakCrypt Crypto Competition	15-Oct-2025 to 30 Oct-2025
Final Round	26-27 Nov, 2025
International Cryptography Winter School	24-26 Nov, 2025
International Cyber Security Symposium	26-27 Nov, 2025
Closing Ceremony Prize Distribution	28 Nov, 2025

✱ Prize Money of at least Rs. 3.0M will be distributed in different competition formats.

✱ For all finalists, registrations in Winter School and Symposium, as well as accommodation will be free of charge.

Our History

PakCrypt competition was initiated in 2022 to promote young talent in the field of cryptography. Last three events of PakCrypt from 2022 to 2024 were great success! It's truly inspiring to see bright minds across Pakistan come together and showcase their talent in the field of cryptography.

Last year, the PakCrypt 2024 competition included more than 900 participants from all regions of Pakistan competing in the three-round competition that culminated in a final round on the NCCS campus. The finalist teams competed for cash prizes totaling Rs. 1.8M, but the competition was much more than this. It provided young minds with opportunities to connect with industry experts, receive job offers, funding for further research, and engage in mutual collaboration.

PakCrypt 2023

FINALISTS
PROFESSIONAL TRACK

248 Participants
16 Finalists

1
Muhammad Abdullah Abid
SAMEEM SHABBIR

2
Muhammad Khurram Hameed
MUHAMMAD USMAN FAZAL AWAN
USAMA MUSADIQ
NASIR ALI
MUHAMMAD SAJJAD
WALEED AHMED
AHSAN RASHEED ABBASI

3
MUHAMMAD BALEEGH UD DIN
Muhammad Umair Aslam
FIZZA BATOOL
SIDRA REHMAN
ARSHAM MUNAWAR GILL
MEHMOOD UL HASSAN
AZAN SHAHID

PakCrypt 2023

FINALISTS
AMATEUR TRACK

292 Participants
24 Finalists

1
FROEBEL — Muhammad Ahmad Bhatti (KHI)
British School — Muhammad Ibrahim Tahir (SGI)

2
Sundar STEM — Syed Badar ul Islam (LHR)
Sundar STEM — Khawaja Assam Arif (LHR)

3
Pak Turk Maarif — Muhammad Safiullah (HYD)
PIEAS — Muhammad Huzaifa

Sundar STEM — Shah Zaib (LHR)
Sundar STEM — Sami Shahbaz (LHR)
Sundar STEM — Abdullah Qayyum (LHR)
Sundar STEM — Muhammad Haseeb Ali Imran (LHR)
Cadet College Hassanabdal — Rayyan Arshad
Cadet College Hassanabdal — Abdullah Tahir
The Science School — Abdullah Aamir
UET Taxila — Iqra Zafar
Siddeeq Public School — Fatima Khalid

The Science School — Muhammad Hammad Ali
Cadet College Hassanabdal — Syed Omer Zakir
Siddeeq Public School — Suleman Nouman
International Islamic University — Faizan Rasheed Abbasi
UET Taxila — Amna Hassan
COMSATS — Irum Imtiaz
COMSATS — Raveeha Naseem
Fast NUCES — Fatima Khan
COMSATS — Manahil Khan

Cash Prizes worth approx. Rs. 1.8M were distributed in 2024, besides a number of career opportunities for selected candidates.

PakCrypt 2024

NCCS — NATIONAL CENTRE FOR CYBER SECURITY

FINALISTS — AMATEUR TRACK

571 Participants
24 Finalists

❶ Karachi Grammar School — Muhammad Ahmad Bhatti
❶ UET Mehran — Muhammad Safiullah
❷ Sundar STEM School — Ahmed Imran Malik
❷ Sundar STEM School — Muhammad Aneeq
❸ LGS — Syed Badar Ul Islam Shah
❸ Sundar STEM School — Khawaja Assam Arif
❹ Aitchison College Lahore — M. Saad Munir
❹ Siddeeq Public School — Sabih Ahmed
❺ Sundar STEM School — Syed Shuja Haider
❺ Sundar STEM School — Sami Shahbaz

M. Ghulam Mohiuddin — Sundar STEM School
Syed Kazim Raza Jafferi — SuperNova School
Hissan Kibria — Cadet College Hassanabdal
Mohammad Arslan — Cadet College Hassanabdal
Muhammad Arhum Shahid — Sundar STEM School
Syed Ali Shah — FAST

Zainab Kayani — FAST
Tooba Naeem — CITY School
Maisha Shaikh — Siddeeq Public School
Abiha Azhar — Siddeeq Public School
Fatima Khalid — Punjab College
Abeeha Noor — KIPS College
Ayesha Salyana — Siddeeq Public School
Wanya Sajjad — Siddeeq Public School

PakCrypt 2024

NCCS — NATIONAL CENTRE FOR CYBER SECURITY

FINALISTS — PROFESSIONAL TRACK

324 Participants
14 Finalists

❶ GIKI — Syed Basim Mehmood
❷ FAST — Mehmood ul Hassan
❸ NASTP — Waleed Ahmed
❹ UET Taxila — Maheen Khalid
❺ Bahria University — Muhammad Ahmed Raza

Mehak Usman — NUST
Nasir Ali — Bahria University
Duaa Aamir — FAST
Muhammad Moarij Ali — FAST
Umer Farooq — FAST
Burhan ud din — FAST
Warda Altaf — Jinnah University
Syeda Afia Shah — UET Peshawar
Muhammad Zeeshan — Islamia University

About PakCrypt 2025 Competition

PakCrypt 2025 is a two-track, three-round competition that comprises both online and on-campus rounds. The competition aims to bring together talented minds of Pakistan around the world to showcase their skills and compete for cash prizes in both professional and amateur tracks.

Round 1: Registration

bit.ly/pc24reg

The first round is open to all Pakistani nationals. It involves a registration process coupled with a screening test. The registration process collects basic information about candidates, while the test serves as an entry-level filter.

Top qualifiers from Round 1 will be announced by the start of October and invited to compete in the second round.

Round 2: Online Competition

The second round of PakCrypt will be conducted online. It is planned to take place in middle of October. Participants who qualify from Round 1 will have the opportunity to display their skills and compete against other talented individuals. The qualifiers of Round 2 will be given opportunity to register for Round 3 as a team of 1-2 persons (both of whom must be Round 3 qualified). Note that prizes will be equally shared among winning team members.

Round 3: On-Campus Final

The final round of PakCrypt 2025 will be held on campus at NCCS, Air University, Islamabad in Nov 2025. The top teams from the previous rounds will compete for the prize and prestige.

Please visit the Crypto Corner at the NCCS website regularly for further details & announcements.

Instructions

△   The registration for Round 1 is estimated to take approximately 30 minutes. It's general math aptitude test. Plan accordingly.

△   The concepts in following resources will help to unlock many riddles of Round 2.
o   Stu Schwartz: Cryptology for Beginners (Amateur)
o   W. Stalling: Cryptography and Network Security 7e and JP Aumasson: Serious Cryptography (Professional)

△   For Round 3, if you are coming out of the twin-cities, there are a number of slots for free accommodation. Please contact the organizers if you are selected for Round 3, at least 2 weeks in advance.

△   No TA / DA is admissible for Round 3 participants, however, food and accommodation may be arranged for qualified top teams. Further, each finalist team that does not fall in top-3 slots will receive an encouragement cash prize.

△   For Amateur Track in Round 3, a teacher of corresponding institute may accompany as part of the student team, however, the teacher will not be allowed to help students in Round 3 challenges.

△   The amount of prize money, allied benefits, and distribution formula will be announced prior to Round 3; At baseline, Rs. 1.7M is already allocated by PakCrypt organizers for prizes.

△ All   Pakistani   nationals,   except   employees   of intelligence/sensitive orgs, are allowed to participate. In case   of   confusion,   contact   PakCrypt   organizers   at 2025@pakcrypt.org

△ For Amateurs, the upper age limit is 20-year.
     (born after 01-Jul-2005)

Sample Questions For Registration
(Amateur and Professional)

Q # 1:- Consider the sequence of numbers: 1, 1, 2, 3, 5, 8, 13, ... and so on. What would be the next number in this sequence?

Q # 2:- What is next?
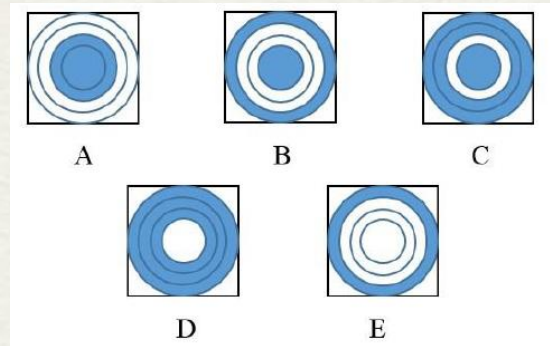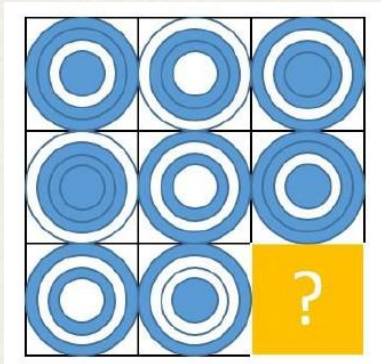
Q # 3:- What is next?
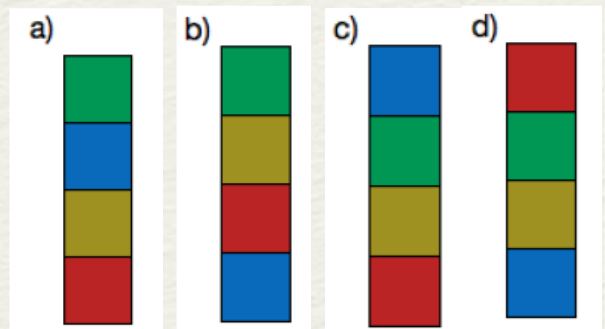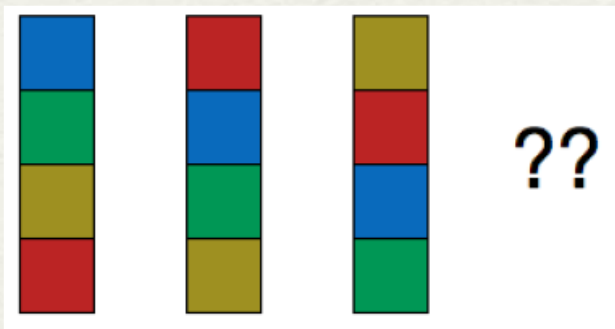
Q # 4:- A bag contains 4 red, 3 blue, and 2 green balls. If a ball is drawn at random from the bag, what is the probability that it is:
a) Red
b) Not Green
c) Blue Or Green

Sample Questions For Registration
(Amateur and Professional)

Q # 5:- A group of friends went on a holiday to a beach resort. They've decided to participate in a relay race where each person can run at a different speed. The group consists of 4 friends: Alice, Bob, Charlie, and David. Here are their respective speeds:

Alice can complete the race in 10 minutes; Bob can complete the race in 15 minutes; Charlie can complete the race in 20 minutes; David can complete the race in 25 minutes
However, due to the rules of the relay race, only two people can run at the same time, and they must carry a baton that they pass on to the next pair. The speed of each pair is determined by the slower person.
Given these conditions:

a) What is the fastest time that all friends can complete the race?
b) What is the order of runners for that fastest time?

Q # 6:- Consider the following statements: "All apples are fruits. No fruit is a vegetable. Some vegetables are green."
Based on these statements (and nothing else), answer the following questions:

a) Are all fruits apples?
b) Can an apple be a vegetable?
c) Are all vegetables green?

Sample Questions
For Round 2 and Final Round (Amateur)

Q # 1:- What is Next?

1	1	2	4
1	2	5	12
2	5	14	37
4	12	37	?

The Answer is 106

Q # 2:- Arrange one of each of the four given numbers, as well as one each of the symbols — (minus), x (times) and + (plus) in every row and column to arrive at the answer at the end of the row or column, making the calculations in the order in which they appear. (Hint:- Only 2,3,7,8 are used)

3	+	8	×	2	-	7	=	15
-		-		+		+		
	+						=	48
+		+		×				
	-	3	+	8	×		=	24
×				-				
	×			7		3	=	12
=		=		=		=		
64		8		33		27		

Sample Questions
For Round 2 and Final Round (Amateur)

Solution:-

3	+	8	×	2	-	7	=	**15**
-		-		+		+		
2	+	7	-	3	×	8	=	48
+		+		×		×		
7	-	3	+	8	×	2	=	24
×		×		-		-		
8	×	2	-	7	+	3	=	12
=		=		=		=		
64		8		33		27		

Q # 3:- A message is hidden in the following maze. What is the message? (Hint: Message starts with FAIL)
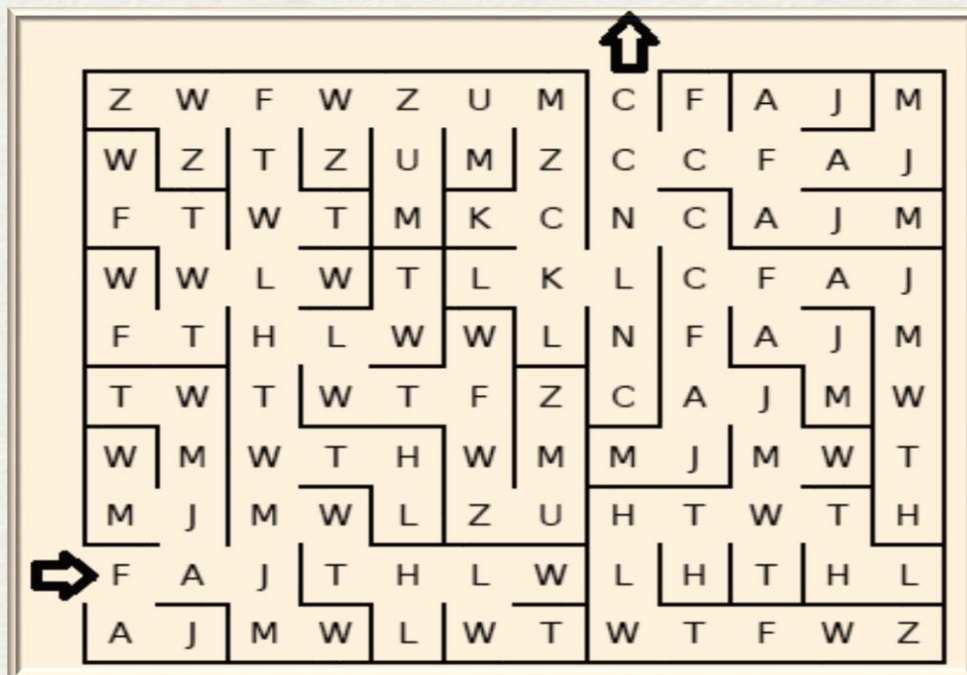
Sample Questions
For Round 2 and Final Round (Amateur)

Solution:- First solve the maze. The answer will be "FAJMWTHLWTFWZUMZCKLNCC". As the message starts with "FAIL", FAJM corresponds to it. It is easy to check that there is no shift in F and A. There is one shift in I and L. Moving Forward, it is easy to judge that the sequence of shifts for letters is 00,11,22,33,44,…… Mapping these shifts will result in "FAILUREISPARTOFSUCCESS"

Q # 4:- An Encryption scheme is provided below.

Keys	A	B	C	D	E	F	G	H	I	J	K	L	M
A,B	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C,D	O	P	Q	R	S	T	U	V	W	X	Y	Z	N
E,F	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
G,H	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
I,J	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
K,L	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
M,N	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
O,P	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
Q,R	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
S,T	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
U,V	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
W,X	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
Y,Z	Z	N	O	P	Q	R	S	T	U	V	W	X	Y

Using the keyword "HELLO", the plaintext "CRYPTOGRAPHY" is encrypted as "SCGKMLVMSIXJ". What is the plaintext for "JTMJLUGWI" with same Keyword?

Solution:- ZEROSEVEN

Sample Questions
For Round 2 and Final Round (Professionals)

Q # 1:- A company has provided public and private RSA keys to all the employees of its organization.

a)   The company boss has used the same value of p, q and thus n to generate the different private and public keys for each employee. Values of p,q are not shared with any employee.

b)   The private key is securely provided to each employee and all the public keys have been posted on the company whatsapp group.

You are one of the employees and your job is to break the system i.e. provided that you have your private and public key and the value of n, find the private key of any other employee (you already have the public keys of all employees).

As an example, we are providing you a sample value of n and one private/public key pair.

N:-

6b81d90c01b573521f728943af7deeffdbf3bf39d4b7b92057d4bbb7e395909d5fd0643aab511fb2f21e9e4bca7a9f2dca5e1afd22328d605566223c0efa0f7e55215f467d4fb88baaf3f11347dff5701a8cda615a489ae95d1eea4fa2aae21a84f5309a1297949a2223c09949f2309e3e1b56c075c2c4593347ba10e74da009

E_{emp1}= 10001

D_{emp1}=

4ad9308007808993597e76a61d180e0310ab5fd610a148fb350f32f6eabe8a9b2a7ceb2b99624f8e8e16127dca4b012bb12b5ca1c8afe9f277ecd88f03f8d21d36a67cfac3ad3458184aec03922f150b79d2f4b3512eb4e042a553e4dd65a9ada6a8bcea2c6505c53e50e2c1dcff3c286419cbba9e15cf3896a717d4dabb3ea01

E_{emp2}= 10111, What is the value of D_{emp2}?

(Note:- Simple RSA is used without any padding schemes)

Sample Questions
For Round 2 and Final Round (Professionals)

Solution:-
1.   Compute k=ed−1 (k is a multiple of Φ(n))
2.   Determine the exponent of 2, t, in the factorization of k, i.e. factor k into the form
$k=2^t r$ with t>0 and r is odd.
3. Pick a random x |2≤x<N
4. Compute the sequence s = $g^{k/2}$, $g^{k/4}$,..., $g^{k/2^t}$ (mod N)
5. Determine the first index i such that $s_i \neq \pm 1$ (but of course its square will be 1)
o If no such index exists, choose a new x and try again.
o Otherwise, let $p=gcd(s_{i-1},N)$ and q=N/p.

Q # 2:- Master Inc. Corporations database server is under attack, the attacker uses the following equation, to encrypt the data:
Ay + 17 *mod* 26
When the attack is complete, the attacker leaves a message flashing on the screen.
"MLKB CRXE NMLV LGRG LNEX BQJB WGGC BNEB XZNP VRDB"
The CERT team is trying their best to make sense of the message, as they believe, it could reveal the identity of attacker, can you help them?

Sample Questions
For Round 2 and Final Round (Professionals)

Solution:- Let

$C = Ay + 17 \bmod 26$

Where, C stands for text appears on screen and x is required text. $C-17 = Ay \bmod 26$ $C-17/A = y \bmod 26$

So, for value of A, the following condition must holds. $gcd(A, 26) = 1$

Hence, possible value of A are $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

For $A=1$:

Equation becomes $(C-17)/1 = y \bmod 26$, $C-17 = y \bmod 26$

Now by putting one by one value of appeared text in above equation, corresponding text is "VUTK ---- ---- ---- ---- ---- ---- ---- ---- ----". It does not show a meaningful text.

For $A=3$:

Equation becomes $(C-17)/3 = y \bmod 26$, $9(C-17) = y \bmod 26$

Now by putting one by one value of appeared text in above equation, corresponding text is "HYPM ---- ---- ---- ---- ---- ---- ---- ---- ----". It does not show a meaningful text.

For $A=5$:

Equation becomes $(C-17)/5 = y \bmod 26$, $21(C-17) = y \bmod 26$

Now by putting one by one value of appeared text in above equation, corresponding text is "ZEJC ---- ---- ---- ---- ---- ---- ---- ---- ----". It does not show a meaningful text.

For $A=7$:

Equation becomes $(C-17)7 = y \bmod 26$, $15(C-17) = y \bmod 26$

Now by putting one by one value of appeared text in above equation, corresponding plain text is "DOZU ---- ---- ---- ---- ---- ---- ---- ---- ----". It does not show a meaningful text.

Sample Questions
For Round 2 and Final Round (Professionals)

Solution Q #2:- For A=9:

Equation becomes $(C-17)/9=y \bmod 26$, $3(C-17)=y \bmod 26$

Now by putting one by one value of appeared text in above equation, corresponding text is "LIFE ---- ---- ---- ---- ---- ---- ---- ---- ----". It shows a meaningful text. So, continuing in this way, get a whole text which is "LIFE HAS NO LIMITATIONS EXCEPT THE ONES YOU MAKE".

Q # 3:- You have been provided with the public key of a fictive person – Ahmed – and a list of intercepted messages. The signedMessages is a list of intercepted messages containing the plain text and the ECDSA signature. The hash of plain Text used for the signature is also provided with the message. Value of q is 503.

```
{
    "name": "Ahmed",
    "publicKey": {
        "x": "82",
        "y": "246"
    },
```

Sample Questions
For Round 2 and Final Round (Professionals)

XV

```
"signedMessages": [{
    "text": "Pakistani",
    "hash": 263,
    "signature": {
        "r": "423",
        "s": "142"        }
}, {

    "text": "Cryptography",
    "hash": 323,
    "signature": {
        "r": "414",
        "s": "390"        }
}, {

    "text": "CryptoC",
    "hash": 114,
    "signature": {
        "r": "469",
        "s": "388"      }
}, {

    "text": "Crypto2024",
    "hash": 362,
    "signature": {
        "r": "56",
        "s": "290"   }
}, {

    "text": "Challenge",
    "hash": 263,
    "signature": {
        "r": "56",
        "s": "243" }
}]
```

Sample Questions
For Round 2 and Final Round (Professionals)

You are required to impersonate Ahmed and sign following messages on his behalf.

Text	Hash
Pakistan	277
Cryptography	227
NCCS	284

Solution:– This is nonce attack. The last two values of signature 'r' are same so they have been generated with the same value of "k".

And we can find it with the formula

$K = (S_4 - S_5)^{-1} * (H(m_4) - H(m_5)) \% q$

Putting the values, we get k= 473

Now the private key can be extracted from the formula of S_4 or S_5 e.g. $S_5 = k^{-1} * (H(m_5) + r * d)$ and it comes out as 431.
 Once you have the private key, it is trivial to sign any message.

PakCrypt Participants' Data Collection and Usage Agreement

By participating in PakCrypt, you agree to the collection and use of your personal information by the PakCrypt Organization Committee for the following purposes:

- Verification of participants for Age / Association / Nationality / Place of Residence / etc.
- Informing participants of PakCrypt Updates
- Distributing prizes to participants in the final round

Personal information will not be shared with any commercial entity or used for any other purposes without your consent.

Disclaimer: The terms and conditions of the PakCrypt Competition, including dates and prize money, are subject to change by the PakCrypt organizers without explicit prior notice. The organizers' selected jury has discretionary powers for decision-making including awarding points and the selection of winners. All media, information, and data in this brochure have been collected and assembled by anonymous volunteers. Therefore, the PakCrypt organizers or NCCS bear no responsibility for copyright infringements or any other similar legal claims.