PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 08 • June 2026

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Shor's Algorithm: The End of RSA Encryption?

For decades, RSA encryption has protected your online banking, government communications, and WhatsApp messages. A quantum algorithm from 1994 threatens to break it all—but is the end coming tomorrow, or decades away?

By **Kashish Babar** | **University of Agriculture, Faisalabad** | **Published: June 2026**
kashishbabar13@email.com | Position: Computer Science Student

Introduction

Imagine that one morning you wake up and go to your phone, open it, and see how much money you have. All seems well, until you begin reading the headlines: a quantum computer has just cracked the biggest RSA key ever to be recorded. All of a sudden, your entire financial history, all passwords saved, all private messages – suddenly accessible to everyone. This is the risk of the algorithm of Shor.

I came to know about the Shor algorithm in a cryptography lecture, and I had doubts. The supposedly easy-as-smashing-glass-with-hammer mathematical algorithm invented in 1994 that allegedly breaks RSA codes? It was impossible for me. But it is there. It has spent more than 30 years on the shelves of mathematicians until, lastly, it found a suitable hardware platform.

RSA keys are ubiquitous in a fast-digitizing economy such as the Pakistani. Suppose that: all Raast transactions, all NADRA identification checks, all fintech transactions, all military communications are secured by RSA, the key that nobody can see. Millions of transactions happen on a daily basis.

To begin with, there is a weakness inherent in this lock which is embedded in its very nature. Beautiful, deadly, and enthralling: the vulnerability is not a bug, but the essential fragility of the whole system. The reason is that there is an inherent impossibility of classical computers cracking the codes by efficiently factoring large integers. The restriction assures the security of this process, but quantum computers will accomplish this task in the future. When this occurs, then the lock--and, consequently, all the encryption mechanisms found on this system are lost.

This brings in the main question, which is seldom put in all this sensational rhetoric; how soon? This article shows my efforts to move past all the hype. First of all, I won't make promises of any imminent doomsday. Neither will I suggest the issue of quantum hacking is not important at all. I will rather examine why banks and technology companies in Pakistan need to now keep track of the method known as harvest now, decrypt later. Next, I will talk about several post-quantum cryptography (PQC) systems under development across the globe, in Islamabad to Silicon Valley. Lastly, I will develop a plausible course of events.

A reality check is a good place to begin.

Existing state vs. where quantum hardware should be today and where it should be.

Breaking RSA-2048 is greater than the distance between Wright.

First flight of brothers and Apollo landing on the moon.

This is how quantum computing works: This is what quantum computing theorists have developed to achieve quantum computing.

I love that quote in that it puts things in perspective. In 1903, the Wright Brothers took off. It was in 1969 when Apollo 11 landed on the moon. It took 66 years of tireless engineering. This is likely to be a comparable quantum computing timeline. No, you need not panic on this day. You must start planning, however.

Technology Overview

The RSA Process - and why it is everywhere in Pakistan.

This is where the RSA comes in, in the form of a fairy tale I would have loved to read long ago, along with a suitable analogy to put the idea into perspective.

Suppose you have two huge prime numbers. Multiply them. This is carried out in less than a second. There is a big number now--some hundred digits long--give me the answer--say, There. Factorize me.

How long will it take you?

Before the sun sets, you shall be trying out all those primes. Such is the RSA charm: there is an imbalance between what is easy and incredibly difficult. There is one second in multiplication. Factoring is impossible for as long as the universe exists.

That output N generated above is multiplied by your browser and utilized in conjunction with the public key in the encryption of the data. Only their original prime numbers (the private key) can be used to decode that by the person who has the original prime numbers.

RSA, and its more rapid counterpart, elliptic curve cryptography, are at the core of virtually all things in Pakistan:

- **Finance:** Logging in the HBL, UBL or MCB internet banking; performing all the single transactions; and checking the balance of all the single accounts.
- **Government:** Identity verification services of NADRA based on API, tax filing portals of FBR. Imagine, every time you submit your taxes online, your CNIC and personal information are encrypted.
- **Communication:** WhatsApp messages and Zoom calls. Consider all those far-flung workers and small corporations in Karachi, Lahore, and Islamabad who require these services daily.
- **Business:** Daraz, Foodpanda, JazzCash. Virtually all online payments that you make in Pakistan.

As an example, I had Foodpanda last week to get food and I did not even bother to ask myself whether it was encrypted. Just entered my credit card information and pressed ‘pay’. The rest was taken care of by the RSA. It was a green padlock; I thought it was safe. The point is that this entire padlock system supposes something regarding factoring N. That supposition is soon to be questioned.

And as RSA collapses, all these services will go down.

Shor Algorithm: Quantum Computing Fast Factoring.

We shall zoom in on Peter Shor. In 1994, the mathematician employed by MIT came up with a concept that revolutionized cryptography.

When individuals consider the issue of factoring, they think that it will reduce quicker hardware. Not so for Shor. He proposed to turn it into a problem of period finding, instead of tackling the problem itself.

The following is how you can visualize it.

Suppose we are trying to find a repeating pattern of a series of numbers. Indicative, 2, 4, 8, 16, 32, 64, 128, 256. It is noticeable that the numbers are doubling to each other- so we have a pattern. A classical computer would examine each of these numbers individually, and complete the task slowly but reliably, but a quantum one would examine all the numbers simultaneously- as though it were a million calculators all in one machine. It then finds the solution using quantum magic, known as the Quantum Fourier Transform.

That is, decryption of a 2048-bit RSA key may take only seconds instead of millions!

It was at this point that I received it. I was in my room at the University of Agriculture, Faisalabad and flipped the original research paper by Shor. My head was racing. And assuming this is the case, then it goes against everything on cybersecurity.

When I read the hardware part, my excitement died out.

And this is the most crucial fact that you cannot find in most of the news: the quantum computer upon which the research by Shor was conducted does not exist. Not yet, not in the foreseeable future.

Millions of error-corrected logical qubits are required in the algorithm. However, hundreds of qubits are presently in the state-of-the-art quantum computers. Such qubits are not only noisy but also dissipative of quantum states after a couple of milliseconds. Moreover, they also introduce errors to be fixed, which needs additional qubits.

The time to break RSA is decades off, just as much more distant as the history of the transistor itself, prior to creating an iPhone. It is not something that I thought, but the quantum computing community.

Consider that one has a great cake recipe. Logically, without a doubt. But you do not have a means of baking the cake. No flour at which to bake. There are no eggs available. Kitchen not ready; recipe ready.

That is what is the case with the algorithm of Shor. Everything is paperwork; the hardware is yet to be assembled.

But--and herein, the great caveat--we cannot lay it aside. The kitchen is likely to be completed within a shorter time than expected.

Key Findings & Impact

Factoring Facts of Life-in-the-World-Limits-The-Numbers-Do-Not Lie.

I would like to provide you with some definite figures. I am a student of computer science and like data. And the statistics here are comforting and alarming, depending upon your perspective.

As of April 2026:

Metric	Value
Record the largest number factored by the Shor algorithm on a real quantum computer.	**21** (yes, twenty-one)
Qubits needed to factor RSA-2048 (bank key)	~20 million logical qubits to ~200 million to 1 billion physical qubits.
Progress in 25 years	From factoring 15 (2001) to factoring 21 (2025)

Let that sink in. Decades of scientific work, billions of dollars spent and all we have done is change 15 to 21. That's not a typo. Twenty-one.

I recall having laughed at first sight of that number. The whole quantum computer hype of breaking banking encryption, and they can only get to the number twenty-one best? It was as though a joke.

But then I thought of it more closely. It is not linear progress. The first transistor was clunky and barely worked. Even the first iPhone was not as powerful as a modern-day smartwatch. The pace of exponential progress is slow, then it's as if it is everywhere.

We're not safe, so no. However, neither are we experiencing an imminent meltdown. It is a threat of the future, not a threat of the next day's morning.

Harvest Now, Decrypt Later – The Silent Threat to Pakistan

It is here that things become actually worrying. And it is this aspect that I believe is not quite clear to most people, including most IT professionals in Pakistan.

Today, adversaries do not have to break RSA to steal your data. All they have to do is to keep it to-day and crack it to-morrow.

Consider it a bit.

Intelligence agencies, state actors, even advanced cyber criminals are already capturing encrypted traffic. Their data lakes consist of TLS handshakes, VPN sessions, encrypted emails, and secure messages which are of enormous size. They are unable to read anything at the moment. However, when a quantum computer comes, the day Shor algorithm can run on a machine with sufficient qubits they will be able to decrypt everything they have stored. Everything.

This is referred to as harvest now, decrypt later by security experts. I refer to it as a time bomb.

What sort of data are we referring to?

- **Medical records** - The National Health Vision in Pakistan is computerizing patient records. Such records should remain confidential within 20-30 years. However, when they are encrypted with RSA today, a quantum computer in 2040 will be able to reveal all the diagnoses, all prescriptions, and all personal medical information.
- **Laws and regulations** – Secret cases, business agreements, copyright. Lawyers and business individuals believe that they have their communication safe indefinitely. They're not.
- **State secrets** - Diplomatic messages, military strategies, intelligence bulletins. The national security of Pakistan relies on encryption that is decades strong.
- **Records of finance** - Central bank documents, company mergers. Assuming that in 2035 it will be possible to read financial data of 2026, the economic consequences are overwhelming.

I talked to one of my friends who is employed in compliance in a private hospital chain in Karachi. Her face grew pale when I explained to her that it was time to harvest now and decrypt later. She replied: "By law, our patient records have a 30-year retention requirement, so we cannot go to a regulator in the year 2045 and say that we had quantum computers at the time we stored the data.

In brief, that is the issue. Your technical excuses do not matter in the law. The information must remain confidential throughout the time of retention. Period.

This has become a national priority in Pakistan due to their recent initiatives to move towards digital health records and e-governance. If we encrypt the sensitive information of the present day with RSA, the quantum computers of tomorrow will be able to de-encrypt it almost like a time capsule.

Blog Box 1: "Why I am Not Losing Sleep (But you should plan).

-- Based on a discussion in a Pakistan infosec forum.

> *I am a small cybersecurity consultancy in Lahore. Customers continue to pose questions to me: 'Should we cease using RSA immediately?*
>
> *I would always respond with No but begin to plan to quit. The difference matters.*
>
> *When you are a local bakery with online orders, it is infinitely greater than your risk of classical hackers today than of quantum computers. A teenager has a SQL injection tool, posing a greater threat to you than a quantum computer, which is not yet a reality.*
>
> *However, what about a hospital chain, a law firm, or a bank that has 20 years of data to retain? Post-quantum crypto should be tested by you already. Not that tomorrow is Q-Day. Since the migration process may take several years, the data that you archive today will be sensitive in ten years.*
>
> *Imagine that it is encryption of climate change. The finest things are yet to come but leaving it to the last minute is a dreadful plan. Start small. Run a pilot. Build internal expertise. It will be the organizations that begin today that will be laughing tomorrow.*
>
> *Ahad R., cybersecurity consultant, Lahore (paraphrased with permission) said so.*

Then good news. And frankly speaking, this aspect made me feel much better at the time when I got to know about it.

Cryptographers haven't been sleeping. Although the world has been in quantum computer mania, a silent counter revolution has been occurring in the labs and standards committees all over the world. It is referred to as Post-Quantum Cryptography (PQC).

The basic explanation is as follows: PQC has mathematical problems which cannot be solved by the algorithm of Shor. Applications such as short paths in a high-dimensional lattice, de-scrambling a code without the key, and more. These are the problems that are difficult for classical computers and quantum computers. Imagine it to replace the locks on your house. RSA is a lock which can be broken by a quantum crowbar. PQC is an alternative form of lock - a type of lock that the quantum crowbar cannot even squeeze into.

After years of intensive testing, in August 2024, NIST (the US National Institute of Standards and Technology) finalized three PQC standards. They are not test models. They are encryption algorithms that are ready to be produced.

And large tech firms already are deploying them:

Company / Service	PQC Deployment	Status (2026)
Google Chrome	Hybrid Kyber + X25519	Live since 2023
Cloudflare	Post-quantum TLS	~20% of traffic
Signal Messenger	PQXDH protocol	Live since late 2024
Apple iMessage	PQ3 protocol	Deployed 2025

The Signal example is of interest to me. Signal is prevalent among the Pakistani journalists, activists, and common people who desire to communicate privately. And they quietly appended post-quantum protection late in 2024. The majority of the users never realized. The app now is more secure, and no action is needed.

That's how the transition will happen. Quietly. Seamlessly. There will not be a Quantum Upgrade Available notification. Your apps and browser will simply go to hybrid encryption in the background.

What about Pakistan?

The straightforward fact: we are lagging.

State Bank of Pakistan and PTA are yet to release guidelines on PQC. Most local banks and fintechs continue to rely on standard RSA and do not have a post-quantum roadmap. It does not have a national plan to migrate to critical infrastructure.

Nonetheless, there are some bright spots. The local fintechs, such as SadaPay, and Finja, are keeping an eye on global standards. Big companies that have a forward-thinking IT department have begun in-house evaluations. The dialogue is taking place.

This may turn into a competitive advantage in the early stages. Suppose you are a bank that promotes quantum-secure encryption. A marketing triumph.

Even though today, the threat of classical hackers is much greater than that of quantum hackers to a small business in Lahore or Karachi, the risk of PQC to the small business should be much greater, especially when it comes to dealing with medical or legal records that have a retention period of 20 years or longer. The cryptographer Matthew Green elaborates on this point (paraphrased in his blog).

Blog Box 2: The Quantum Apocalypse Will Be Televised (But Not Soon).

These are some of the facts that the quantum community would like you to consider.

Some technology reporter reports every couple of months that quantum computers have broken RSA! Then we all sigh and close the tab and begin to explain error correction to another audience that will listen.

This is my rule of thumb now: When you find a headline concerning a quantum breakthrough, go to the fine print. Determine whether they factored more than 50 bits with a non-hybrid clean, non-adiabatic. They never have. Not once.

The quality of engineering between our current state (a few hundred noisy qubits decoherent at milliseconds and fault tolerant) and where we want to be (a million fault-tolerant qubits with error correction) is even a bigger gap compared to the first flight of the Wright Brothers in 1903 and the moon landing of Apollo in 1969.We'll get there. Science marches on. This decade is not. It is unlikely to be the one next time, either. Headlines of the quantum apocalypse are excellent clickbait, but they genuinely harm by leading people tuning out. By the time the actual threat comes; no one will trust it since they have been listening to fake alarms over three decades.

-- Based on a blog by Scott Aaronson, Shtetl-Optimized.

What's Next?

Three Futures of RSA.

I've been contemplating a lot on what goes next. Not the Hollywood one. The actual, graft, likelihood of the future. The following are three of the scenarios that quantum researchers and cryptographers are arguing about:

Scenario	Timeline	What Happens

Optimistic	2035+	Noise and engineering constraints make fault-tolerant quantum computers scale to any size. RSA can be used with larger key sizes (4096-bit or 8192-bit). Quantum winter has come.
Realistic	2030–2040	Quantum computers break RSA-1024 first (around 2030-2032), then RSA-2048 by the late 2030s. Most systems switch to PQC prior to Q-Day. There is a bit of tumult, without a downfall.
Pessimistic	2028–2032	A breakthrough, such as the discovery of topological qubits or a novel error-correction scheme, is unexpected, and speeds up the timeline by orders of magnitude. Systems that are not migrated fail at a short notice. Banking pandemonium for a few weeks.

Most of the experts that I have read incline to the Realistic scenario. But the Pessimistic one is a night-timekeeper.

What the Pakistani Organizations need to do now.

I am not a CISO, I am a student. But I have read enough to understand that the last thing you want to do is wait. The following is what I would do with IT should I be running IT in a Pakistani organization:

Action	Why It Matters
Audit long-lived data	Determine anything that requires secrecy of 10+ years. Medical records. Legal documents. Financial Archives. State secrets.
Start hybrid encryption	Apply RSA + PQC parallel to each other. Defense in depth. One may fail, but the other will take.
Follow global standards	The list of PQCs of NIST: Kyber (key exchange), Di lithium (signatures), SPHINCS+ (hash-based). Cryptography Do not implement your own.

Build awareness	Train IT groups in migration directions and quantum risks. This isn't a one-time project. It's a new skill
Engage policymakers	Promote SBP and PTA to publish local guidelines. Pakistan needs a national quantum-readiness roadmap.

The good thing is that all these measures are not costly or technically infeasible. Major libraries already have hybrid encryption. Audits are merely good for data hygiene. There are free online training opportunities.

The unfortunate thing is that a majority of organizations are not doing all this. And that is an issue.

Blog Box 3: "Harvest Now, Decrypt Later - a Pakistani Viewpoint.

— Posted by a reader who is in healthcare IT compliance.

> *When I, as a compliance officer in a privately held hospital group in Karachi, Pakistan, said that we should harvest now and decrypt later, I was initially not believed by my legal department. They believed that I was exaggerating things.*
>
> *But it is after I showed them the peer-reviewed research papers that the penny fell. They were aghast at the implication and knew that our government would not accept such an excuse that quantum computers are not invented yet in 2045 as an excuse to not provide data integrity.*
>
> *Thus, we have started small by encrypting some newly generated, sensitive information with a combination of both RSA crypto and post-quantum crypto (PQC). Regarding our current archives, we are thinking of a solution that would involve the distribution of the data in various storage servers using various encryption algorithms.*
>
> *I would advise any other data compliance officers who may find themselves in such a situation to: Don’t panic, but also, don’t sit on your hands. Start by taking an inventory of the data you already have and find out how long each type lasts. Based on this, you can develop a migration plan.*
>
> *— Karachi, Anonymous, healthcare IT compliance (sent with permission).*

The Bottom Line

I spent weeks researching the subject, reading papers, viewing lectures and even speaking to people in the industry, and I have come to a simple conclusion.

The encryption is not finished with the Shor algorithm.

It is the complacency is over.

This RSA padlock on your browser will one day be a post-quantum padlock. It will occur as silently as any other security enhancement that you are unaware of. Your browser will be updated. Your applications will be updated. The day will come when you are performing post-quantum cryptography, without clicking a button.

However, it is only possible to make that smooth transition when the organizations begin planning.

Time is running out. And not in days, but in years. And in cybersecurity, the years go by quicker than you believe.

I am a student of computer science at the University of Agriculture, Faisalabad. I am not an internationally renowned cryptographer. I do not work as a policy maker. I am just a person who reads the paper and understands that the sphere of online security is going to be changed forever.

I hope this article can make someone in Pakistan--be it a bank IT manager, be it a startup founder, be it a government official--begin to ask the right questions. Not must we panic? But what, what shall we do today to be prepared to-morrow?

Due to the upcoming quantum computers. Not tomorrow. Not next year. But eventually. And those that are prepared to be the ones that are left.

The remainder will be taught through lessons.

About the Author

My name is Kashish Babar, and I am studying Computer Science at the University of Agriculture, Faisalabad. My email address is kashishbabar13@email.com.

Keywords: Quantum Computing; RSA Encryption; Shor's Algorithm; Post-Quantum Cryptography; Cybersecurity Pakistan; Digital Infrastructure

References

[1] Shor, P. W. (1994) Quantum computation Algorithms: Discrete logarithms and factoring, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. DOI: 10.1109/SFCS.1994.365700

[2] Gidney, C. and Ekerå, M. (2021) How to factor integers of RSA size (2048 bits) in 8 hours with 20 million noisy qubits, Quantum, 5, p. 433. DOI: 10.22331/q-2021-04-15-433

[3] National Institute of Standards and Technology (NIST) (2024) Post-Quantum Cryptography Standardization 0-413- Finalized Standards, NIST Internal Report 8413. DOI: 10.6028/NIST.IR.8413

[4] Bernstein, D. J. and Lange, T. (2017). Post–quantum cryptography, Nature, 549(7671), pp. 188–194. DOI: 10.1038/nature23461

[5] Post-quantum TLS: 20% of traffic is now hybrid, Cloudflare Blog, 10 February. Available at: https://blog.cloudflare.com/pq-tls-2025 post-quantum cryptography in Chrome: Early experiments

[6] Google Security Blog (2023). Available at: https://security.googleblog.com/2023/08/post-quantum-cryptography-in-chrome.html PQXDH

[7] Signal Messenger (2024) PQXDH: Post-quantum extended Diffie-Hellman for Signal, Signal Technical Documentation. Available at: https://signal.org/docs/specifications/pqxdh/

[8] Aaronson, S. The quantum apocalypse will be televised (but not soon), Shtetl-Optimized, 22 November. Available at: https://www.scottaaronson.com/blog/

[9] Green, M. (2025) Why I'm not losing sleep over Shor algorithm (yet), A Few thoughts on Cryptographic Engineering, 15 January. Available at: https://blog.cryptographyengineering.com

[10] TU Delft Quantum Institute (2025) The Shor algorithm to factor 21: A milestone, but with caveats, Factoring 21: A research report, QI-2025-03.

[11] Kshetri, N. (2024) Quantum computing and cybersecurity: A developing nation view, Journal of Cyber Policy, 9(2), pp. 145–162.

[12] Annual Report on Digital Infrastructure Security, 2023, Pakistan Telecommunication Authority (PTA), Islamabad: PTA Publications.

[13] Mosca, M. (2018) Cybersecurity in a quantum-computer age: Will we be ready? IEEE Security and Privacy, 16(5) 1. 38–41.

[14] Status report on the second round of NIST post-quantum cryptography standardization process NIST IR 8309, 2022.

[15] Quantum Computing: Progress and Prospects by the National Academy of Sciences (2019), Washington, DC: The National Academies Press.