PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 16 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

# The Invisible Shield: How Data Encryption can keep the Digital World safe

*You can use encryption in the background every time you tap to pay, log in to your bank, or send a one-way message. Knowing about it has ceased to be a prerogative of IT departments, it has become a prerequisite to anyone in the modern digital environment.*

By **Muhammad Dawood Arif** | Department of computer Science | Published: August 2026
dawoodarif462@gmail.com

## Introduction

Take the case of writing a letter, putting it in an envelope, in which the only person who can access the letter is the recipient, and sending it across a city full of strangers who may intercept the letter at any point. That is basically what data encryption does namely; except that the city is the internet, the strangers are hackers, and what is at stake are your money, your identity and the existence of your organisation.

Data breaches have turned into one of the most characteristic disasters of the digital era. Hackers are no longer working alone in the dark rooms; they now operate organised networks where the stolen credentials are sold in the underground markets and malware programs deployed so as to cripple hospitals, banks and government agencies within a few hours. Within this setting, encryption will no longer be a technical nicety. It is the last line of defense.

The power of encryption that is often misconstrued is the fact that encryption does not prevent an attacker gaining access to your data. It just makes sure that anything that they discover is absolutely worthless to them. A properly encrypted file is not noise: a meaningless sequence of characters that, in the absence of the relevant decryption key, is just noise. And there the main guarantee of the modern cryptography, and there the guarantee that in the proper implementation it can be held even against advanced enemies.

> ***" That is the pledge, and when it is properly carried out each of us, even when we are against a highly developed opponent, will find that that promise holds even when properly implemented."***

## An explanation of how Encryption really works and why it comes in various flavours

Fundamentally, encryption is a mathematical transformation. It encrypts readable information, such as a password, a bank record, a personal message, etc. and encrypts it using an algorithm and a key, resulting in encrypted data that cannot be understood without a key. The reverse process can only be reversed by an individual with the right decryption key and the original data can be retrieved.

Broadly, the active encryption of today is divided into two broad families (symmetric and asymmetric). In symmetric encryption, the same key is employed to encrypt and decrypt the data. It is quick and effective and is hence suitable in encrypting large amounts of data. In asymmetric encryption, two keys that are mathematically linked are used; a public key that any party may use to encrypt the data and a private key only known by the recipient to decrypt the data.

This is the functioning of secure websites: your browser encrypts the information with the public key of a site, and it can be read only by the server of a particular site. Among these two families are some of the well

established algorithms, each having its own personality. The gold standard of symmetric encryption as of today is the Advanced Encryption Standard, or AES.

Implemented by governments and companies all over the globe, it encrypts data in blocks and uses key lengths of 128, 192, or 256 bits - lengths so large that, with the current computing capabilities, they will be more difficult to brutally force. It secures all the things such as the content of operating on a hard drive, conversations in messaging applications. The most popular asymmetric algorithm, RSA, has been securing the web since the late 1970s.

Whenever you look at a padlock in the address bar of your browser, RSA is involved in the handshake that created the secure connection. Its security lies in a most exquisitely simple mathematical fact: it is trivial to multiply together two enormous prime numbers, and it is computationally extraordinary hard to factor the result back into its component parts. Older symmetric algorithms, such as blowfish and Twofish, are still in active use in password managers and file encryption tools, and are also highly valued due to being fast and the fact that they are absolutely free to use, no licensing needed.

The DES, or Data Encryption Standard, is to a great extent an artefact of the past today. Practically its short key length rendered it breakable in modern hardware, and even its successor Triple DES has been phased out in most serious security applications. It is a good reminder that encryption algorithms do not last indefinitely, and there is no such thing as staying up to date.


*Figure 1: A side-by-side illustration of symmetric and asymmetric encryption flows, showing how keys are generated, shared, and used to protect data in transit. Credit: PakTech Today*

## The Threats This Encryption Protects Against - and the ones that it cannot

Encryption is resistant to a great variety of contemporary threats, but it is equally important to understand its limitations as much as it is to understand its advantages. One of the most catastrophic attacks of our time is ransomware - malware that encrypts the files of an organisation and demands a ransom payment in order to decrypt the files.

The ironical cruelty is that the system of encryption that protects us against ransomware is the same kind of the system that ransomware protects against. Attackers encrypt your data using their own key, and lock you out until you pay. Defence is not better encryption, it is normal encrypted backups that are kept apart, so that even when attackers lock your live systems, your data is not lost.

SQL injection attacks are direct attacks on databases, where malicious code is snuck into queries to steal or corrupt database data. The damage can be limited by encryption of stored data: even when an attacker has stolen a database of records, properly encrypted fields - passwords hashed with strong algorithms, sensitive fields encrypted at rest - yield no useful information. A different group of issues altogether are social engineering and phishing.

These attacks are not able to overcome encryption; they bypass it. One of the phishing emails deceives an employee into giving over his or her login details. As long as an attacker has legitimate credentials, then they can access your systems as a legitimate user, and the encryption that might prevent an outsider access is no longer relevant because he is now a legitimate user.

It is here that the policy of encryption and human behaviour come together and where many organisations fail. The simplest part is to install strong encryption algorithms. The difficult part is to ensure that data is always encrypted, at rest, in transit, and in backups, and to ensure that the keys themselves are stored securely.

An encryption key that is not managed well is like a lock that is perfect and the key is taped to the door. This is further enhanced by insider threats. A considerable percentage of the number of data breaches can be attributed to negligence, ignorance or intent on the part of employees.

As important as the algorithms themselves is training on why encryption policies exist, and making it easy for them to follow the encryption policies. Laws and regulations globally have now introduced the use of encryption as a minimum requirement. Minimal standards of the protection of sensitive data are established in GDPR in Europe, HIPAA in healthcare, and PCI-DSS in payment processing. In the case of organizations that operate over borders, adherence to more than one framework at a time is gradually becoming the norm and not the exception. Non-compliance will result in financial fines yet the reputational harm of a breach that is publicised is likely to cost much more.

## The Next Frontier: Quantum Computing and the Future of Encryption

The encryption algorithms which help to protect the data of the world today are built to serve a world of classical computers. The quantum computers will work on entirely different principles, and once they become powerful enough, they will be able to crack the RSA and other similar public-key algorithms in a fraction of the time that it would otherwise require conventional machines. It is not far off theoretical worry.

In 2024, the US National Institute of Standards and Technology has finalized its first wave of post-quantum cryptography standards - new algorithms specifically designed to resist quantum attacks. CRYSTALS-Kyber deals with key encapsulation; CRYSTALS-Dilithium with digital signatures. They are both designed to be secure even with adversaries using quantum hardware.

Proactive organizations are in the process of auditing their cryptographic dependencies, finding out which systems are dependent on RSA or elliptic curve cryptography and are starting to think about migration paths. This is referred to as cryptographic agility and is less about providing an immediate substitution and more about creating systems that are flexible enough to allow replacement of algorithms when the time comes. Another new technology, homomorphic encryption, puts the notion in a completely new perspective.

Instead of having to encrypt data and decrypt it to process it, homomorphic encryption has the capability to have the computations be performed directly on the encrypted data, i.e., a cloud service can be used to process your sensitive records without ever seeing them. It is still computationally costly today, but the trend toward improvement is steep, and practical usage is anticipated in the next decade.

Data encryption has been referred to by various terms such as a technical security measure, a regulatory necessity, and a competitive advantage. It is all of these. But at the most basic level it is a declaration of intent;

that the information entrusted to an organization will be approached with the seriousness to which it is entitled. There are real, increasing, and not waiting threats.

Encryption will not solve the entire problem, but there is nothing of significance that can be achieved without it. Those organizations and individuals who grasp this, and work on it are the ones that will sail into the digital future with the confidence needed.

**About the Author**
Muhammad Dawood Arif is a student of university Of Agriculture Faisalabad.

**Keywords:** Data Encryption; AES; RSA; Cybersecurity; Post-Quantum Cryptography; Information Security; Ransomware; Data Protection

## References

**[1]** **NIST** (2024) Post-Quantum Cryptography Standards. *National Institute of Standards and Technology.* Available at: csrc.nist.gov/projects/post-quantum-cryptography

**[2]** *McGovern, W. (2018) The Duty of Data Security, Minnesota Law Review, 103, p. 1135.*

**[3]** *European Parliament (2016) General Data Protection Regulation (GDPR), Official Journal of the European Union, L 119.*

**[4]** *Alaya, B., Laouamer, L. and Msilini, N. (2020) Homomorphic Encryption Systems Statement: Trends and Challenges, Computer Science Review, 36, p. 100235.*