**DATA ENCRYPTION IMPLEMENTATION EVALUATION**

**VERIFACTS SERVICES PRIVATE LIMITED**

# What is data encryption?

Data encryption consists of hiding information from malicious actors or anyone else with prying eyes.

Data is information. It can be an email message, the contents of a database, or a file stored on a laptop.

We encrypt data to keep it confidential. Data encryption is part of a broader class of cybersecurity countermeasures known as data security. Data security is all about keeping our data safe from unauthorized access, ransomware lockup (which is a malicious form of encryption), breach, or malicious corruption, i.e., changing data to make it useless.

# How does data encryption work?

Modern data encryption is a form of cryptography, an ancient technique of hiding information by substituting one character for another. The word ‘encryption’ is a blend of English and Greek that means “in hidden” or, more loosely, “in hiding.”. Encryption works through a complex mathematical algorithm known as a data encryption cipher. Like the secret decoder ring found in your child’s cereal box, the cipher algorithm transforms normalized data (i.e., plaintext) into a sequence of ostensibly random, unrecognizable characters known as “cipher text.”

The cipher text is unreadable. For example, the phrase, “Hi, how are you?” might encrypt into a cipher text that reads, “8363, 5017, 11884, 9546.” To get back to “Hi, how are you” requires a process of decryption.

Decoding information from cipher text to plaintext is called decryption and involves the same algorithmic “key” that data encryption uses.

# Who needs to use data encryption?

The answer is just about anyone. We don’t have to be a secret agent to want to keep our data confidential. In fact, we might be using encryption without even knowing it. Many technology services encrypt and decrypt our data so it will be safe when they use it. Businesses should encrypt data that could damage their financial results if it were breached. Individuals should encrypt sensitive personal data like their medical histories and social security numbers.

# Benefits of data encryption

**Data Integrity:** By seeing any changes or corruption in encrypted data, encryption helps maintain data integrity and enables a swift response to potential fraud.

**Device Protection:** By reducing the risks involved with data transfer and adding an extra layer of security through sophisticated authentication procedures, encryption technology protects data across many devices.

**Remote Office Security:** With increased remote work, encryption helps protect data from theft or unintentional loss.

**Regulatory Compliance:** To ensure that customer data is handled and stored safely, encryption helps organizations comply with rules particular to their industry.

**Cloud Data Security**: When data is transferred to cloud storage, privacy is guaranteed by encrypted storage.

**Intellectual Property Protection:** Data encryption protects intellectual property like music or software by preventing unlawful use, duplication, or reverse engineering, especially when used with digital rights management systems.

# Common data encryption types

Over the most common data encryption types. The two most widely used methods for data encryption are public key, also known as asymmetric encryption, and private key, or symmetric encryption. Both rely on key pairs but differ in how the sending and receiving parties share the keys and handle the encrypt/decrypt process.

**Public key encryption - asymmetric encryption**

With public-key/asymmetric encryption, the sender uses a publicly known key to encrypt the data. The receiver has the private key that forms the other half of the public/private key pair. The receiver can decrypt the data by using the private key in combination with the public key.

**Private key encryption - symmetric encryption**

In Private key/symmetric encryption, both sender and receiver have the same, secret key. As we might imagine, there’s a lot of management overhead involved in storing and transmitting secret keys.

# Common data encryption algorithms

Companies, encryption products, and government agencies make use of several different encryption algorithms today. These include:

**DES (Data Encryption Standard)**

It's a symmetric key algorithm that played a very relevant role in the history of data encryption. I was developed in the 1970s, becoming widely adopted as a cryptographic standard for securing information. It operates on 64-bit data blocks and employs a 56-bit key size, which was considered robust at the time of its creation. However, due to advances in computing power and the emergence of more sophisticated attacks, the DES algorithm is now considered relatively weak in terms of security.

**Triple DES (3DES)**

An encryption algorithm that provides enhanced security by applying the Data Encryption Standard (DES) algorithm multiple times in a cascading fashion. Each round consists of an encryption, a decryption, and another encryption operation. This triple-layered approach significantly increases the key length to 112 or 168 bits, making it more resistant to attacks and other cryptographic vulnerabilities. Despite its improvements, 3DES is gradually being phased out in favor of more advanced encryption algorithms.

**Advanced Encryption Standard (AES)**

A widely used symmetric key algorithm that has become the standard for securing sensitive data. Based on the Rijandael block cipher, AES offers a high level of security and efficiency. It operates on fixed-size data blocks, typically 128 bits, and supports key sizes of 128, 192, and 256 bits. In addition, it uses substitution, permutation, and mixing operations for robust encryption. It is used in the US federal government and in consumer technologies like the Apple Macintosh computer.

**RSA**

One of the first and most widely adopted modes of asymmetric cryptography for data in transit. It originated in 1977. RSA is based on the mathematical properties of prime numbers and modular arithmetic. It utilizes two keys: a public key for encryption and a private key for decryption. The strength of RSA lies in the fact that even if we know the public key, it is still infeasible to derive the private one.

**Elliptic curve cryptography (ECC)**

A powerful and advanced encryption algorithm that leverages the mathematical properties of elliptic curves. It offers a high level of security while using shorter key lengths, which makes ECC particularly suitable for resource-limited scenarios. Thanks to smaller key sizes, it provides faster computations, reduced memory requirements, and decreased bandwidth usage, so government agencies like the NSA favor it.

**Twofish**

It is a highly secure symmetric key block cipher. It is known for its strong resistance against various cryptographic attacks. It operates on 128-bit data blocks and supports key sizes ranging from 128 to 256 bits, making it flexible and adaptable to different security requirements. In addition, it employs a complex key schedule, multiple rounds of substitution and permutation operations, and a carefully designed Feistel network structure, all of which contribute to its robustness and resilience against attacks.

# How to encrypt your data

We might wonder about actionable steps for basic data encryption on our devices. The good news is that many solutions are available at low or no cost. Android phones have full-device encryption if they run Android Gingerbread (2.3.x) or later. On Pixel Phones and Nexus 5+, encryption is by default. We have to turn it on earlier versions of Android, but it’s there. Setting up encryption on an Android device involves configuring a lock screen PIN, pattern, or password. Then in Settings/App Settings, We choose Security & Location. Where it says “Encryption” on this screen, select “Encrypt Phone.” That’s all it takes. We can do this process in reverse-to-end encryption.

For our computer, we can encrypt our data at rest with solutions from companies like Symantec, Kaspersky, Sophos, and ESET. We can also get encrypted USB drives. In addition, email can be encrypted through products like DataMotion SecureMail software, Proofpoint Email Encryption, and Symantec Desktop Email Encryption.

# Data encryption best practices

**Protect your encryption key**

Although it should be very clear, it's possible to make mistakes that give unauthorized people access to our data. For instance, there is a considerable risk that someone may uncover our encryption key and cause havoc if we leave it in an unencrypted file on our computer. A few alternatives include:

* Keeping the keys distinct from the data
* Separating user roles and access restrictions
* Rotating our keys periodically.

**Evaluate data encryption**

Making our data unreadable to unauthorized parties is only one aspect of effective data encryption; another is doing so in a way that makes good use of the available resources. Consider using a new algorithm or playing with the parameters in our data encryption tools if encrypting our data takes too long or uses too much CPU and memory.

**Encrypt all sensitive data types**

This should also be obvious, but if we read the headlines about IT security, we are aware that many reputable businesses have been compromised simply because they left sensitive data unencrypted and allowed someone else to access it. Encrypting our data makes it much more difficult for someone who can hack into our systems to do bad things.

**Can encrypted data be hacked?**

Encrypted data can indeed be hacked or cracked. Still, the feasibility and difficulty of doing so depend on several factors, including the strength of the encryption algorithm, the length and complexity of the encryption key, and the resources available to the attacker.

There are two main types of attacks that can be used to attempt to compromise encrypted data:

**Brute Force Attacks:** In a brute force attack, an attacker systematically tries all possible combinations of encryption keys until the correct one is found. The effectiveness of a brute force attack depends on the length and complexity of the encryption key. The longer and more complex the key, the more difficult it becomes to crack the encryption using brute force. Modern encryption algorithms often use long keys designed to withstand brute-force attacks.

**Cryptanalysis Attacks:** Cryptanalysis involves analyzing the encryption algorithm itself to discover vulnerabilities that can be exploited to decrypt the data without the encryption key. If a weakness is found in the algorithm, it may become possible to decrypt the data more efficiently than by brute force. This is why it's crucial to use well-vetted and widely accepted encryption algorithms.

In practice, strong encryption algorithms with sufficiently long and complex keys are extremely difficult to crack using these methods. However, there have been cases where encryption has been compromised due to implementation flaws, key management issues, or advances in computational power.

It's important to note that the security of encrypted data also depends on factors such as the protection of encryption keys, proper implementation of encryption protocols, and safeguarding against side-channel attacks (where information is leaked through unintended channels like power consumption or timing).

As technology advances, it's important to stay informed about encryption best practices and to regularly update encryption methods to stay ahead of potential threats.

# The future of data encryption

Data encryption and data security are constantly evolving to keep up with a worsening threat environment. While brute force decryption may be hard, hackers can still steal keys or attack places where encryption is suspended in the data management chain. For example, data is almost always encrypted through a computer’s Central Processing Unit (CPU). This is changing now, with chip makers like Intel introducing encryption tools for their CPUs.

The future of data encryption promises more innovations. These include encryption algorithms that incorporate biometrics and voice recognition—a sort of unique personal key. The industry is also introducing “Honey Encryption” traps that show a fake but plausible plaintext when a hacker guesses at the decryption key. Blockchain, which is not, strictly speaking, a form of encryption, makes use of encryption-like algorithms to ensure the integrity of data that is stored using a blockchain framework. There is likely to be a lot more of this kind coming in the future.

# Using Prey to encrypt your data

Using the Prey Control Panel, We can control BitLocker for disk encryption on Windows 10 Professional, Enterprise, or Education editions, as long as a physical Trusted Platform Module (TPM) is installed and active. This feature lets us choose the specific disk we want to encrypt, monitor the encryption progress, and select your desired security standard from options such as AES128 and XTS\_AES128. Simplifying disk encryption management, Prey empowers us to enhance the security of our Windows system effortlessly.

# Conclusion

In conclusion, data encryption is a vital protection for sensitive information, ensuring data security. Throughout this article, we have dived into the intricacies of data encryption, emphasizing the need to protect confidential data.

While data encryption may require advanced technology, the availability of user-friendly solutions has made it more accessible, particularly for consumers. Encryption is seamlessly integrated into certain systems like iOS, strengthening data protection without user intervention.

For every organization, encryption should be an integral component of their security framework, preserving the integrity of business-sensitive data. Data encryption is an essential tool in our cybersecurity arsenal, and its adoption should be a priority.