

Office of Technology Strategies (TS), Architecture, Strategy & Design (ASD)

A VA Executive's Guide to Encryption

INTRODUCTION

This TS Note discusses encryption, which is the process of encoding data so that only authorized individuals can access it. Encryption is one component of cryptography—the science of secret communication—and the most effective way to secure data. In an encryption scheme, an algorithm encrypts the message, referred to as plaintext, by scrambling it into a random series of letters, numbers, and symbols. This generates ciphertext, which can only be read if decrypted. In an encryption scheme, the algorithm usually generates a pseudo-random encryption key, which enables authorized recipients to decrypt the message.

OVERVIEW

Encryption dates back to the use of hieroglyphics in ancient Egypt. Militaries and governments have used it for centuries to facilitate secret communication, and civilian systems currently use it to protect information and messages (text, binary files, or documents). The two techniques for encrypting information are symmetric encryption (also called secret key encryption) and asymmetric encryption (also called public key encryption).

In a symmetric-key scheme, a secret key (e.g., a number, word, string of letters, etc.) is applied to a message's text in order to change the content. This change could be shifting each letter a few places in the alphabet, or it might be completely scrambling the text. In this type of encryption, the encryption and decryption keys are the same, so the receiver and sender can encrypt and decrypt all messages that use those keys.

In asymmetric encryption, a public key is available to anyone sending a message, while a private key is available only to the receiver. A Certificate Authority (CA) distributes the security credentials and public key after verifying the information provided by the requestor of a digital certificate. Messages that are encrypted with the public key can only be decrypted by applying the same algorithm using the matching private key. Similarly, messages encrypted with the private key can only be decrypted with the public key. This eliminates the risk associated with passing public keys over the Internet, but it is slower than symmetric encryption.

Defining OI&T's
"To Be"
Technology
Vision



The TS office within OI&T's Architecture, Strategy & Design (ASD) interacts not only with the ASD pillar offices, but also with multiple stakeholders within OI&T and with strategic offices across the enterprise. TS works closely with IT and business owners to capture business rules and provide technical guidance as it relates to Data Sharing across the enterprise, specifically for interagency operability.

There are several types of data encryption, which include:

- File and Folder Encryption – Allows users to encrypt files or folders residing on PCs, laptops, or portable storage devices.
- E-mail Encryption – Protects e-mail messages as they travel within and beyond corporate networks.
- Full-Disk Encryption – Encrypts an entire hard drive rather than individual files or messages and is beneficial for those teleworking with laptops.
- Mobile Data Encryption – Encrypts data stored on PDAs and smart phones; e-mail encryption is also used by mobile devices.
- Application Encryption – Encrypts data stored within a custom application (e.g., a payroll system).

DIGITAL DATA STATES

There are three states of digital data: Data in Use, Data in Transit, and Data at Rest. Data in Use refers to data being processed by a computer central processing unit or in random access memory (also referred to as main memory or simply memory).

Data in Transit encompasses both information that flows over a public or untrusted network—such as the Internet or mobile devices—and data which flows in the con-

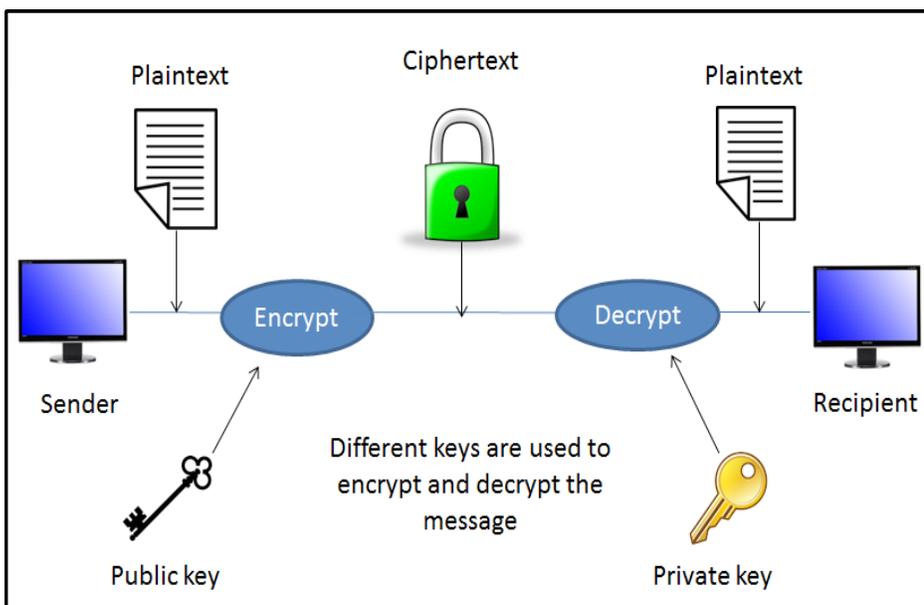


Figure 1: Public Key (Asymmetric) Encryption

A VA Executive's Guide to Encryption

Continued from Page 1

of a private network—such as a corporate or enterprise Local Area Network (LAN). Since this data is accessed over a network, encryption is necessary to prevent interception and eavesdropping by unauthorized users. On an Ethernet network, an unauthorized user is anyone with the ability to tap a cable, configure a switch to mirror traffic, or fool a router into directing traffic to them. On an open wireless network (e.g., in a coffee shop or hotel), anyone within range can access the network's data, unless all traffic is encrypted. Strong enterprise networks can use WPA2 Enterprise to encrypt traffic, but weaker networks may only have pre-shared keys to establish session keys (e.g., WPA Personal). Encrypting Data in Transit is essential in order to protect network traffic that requires authentication or that is not publicly accessible.

As opposed to Data in Transit, Data at Rest refers to inactive data stored in a digital form (e.g., USB flash drives, spreadsheets, archives, etc.). This data is safe as long as it remains physically secure, but reports of confidential data—like customers' personal records—being exposed through loss or theft of laptops or backup drives are increasingly common. Encrypting these files protects them in cases where physical security measures fail.

BENEFITS AND CHALLENGES

The above sections mention a few of the reasons why encryption is beneficial for governments, businesses, and individuals alike. Aside from providing peace of mind, encryption ensures secure communication by allowing users to:

- **Protect Data Completely** – Securely encrypted data is completely protected if stolen. Many encryption keys would take a hacker more than a lifetime to crack.
- **Achieve Security On All Devices** – As the use of mobile devices and tablets grows, data is being distributed across many devices. Encryption ensures that data remains secure regardless of the device on which it is stored.
- **Transmit Securely** – Users sending files over email or on a cloud server can prevent unauthorized users from gaining access.
- **Guarantee Data Integrity** – If encrypted data is manipulated, the recipient will know that it has been tampered with. Targeted data theft is one thing, but another way to misuse data is through manipulation.
- **Ensure Compliance** – Encrypting data is often the easiest way to comply with legal or contractual regulations on data protection.

While encryption provides many useful services to data users, there are still areas for concern when it comes to encrypting data. These challenges include:

- Applications that have legitimate access rights but are infected with malware can still access confidential data.

- If keys are not isolated in a key management system, the wrong individuals can access both encrypted data and encryption keys and gain access to plaintext data.
- Users with broad access rights can disable encryption controls unless proper checks and balances are in place.
- There are high costs associated with providing and rotating keys to multiple users.
- Lost keys render data inaccessible.

ENCRYPTION AND VA'S CURRENT TECHNOLOGY STATE

VA Handbook 6500 states that, "All VA employees, contractors, business partners, and any person who has access to and stores VA sensitive information must have permission from a supervisor and ISO to use removable storage media/devices to store sensitive information." VA is committed to protecting sensitive information through the Federal Information Processing Standard (FIPS) Publication 140-2.

This publication, titled "Security Requirements for Cryptographic Modules," is a U.S. government computer security standard used to accredit cryptographic modules. The National Institute of Standards and Technology issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules. To minimize the risk associated with wireless, mobile, and portable devices, VA requires FIPS 140-2 encryption of information transmitted to and from a wireless device, unless an appropriate waiver has been approved by the CIO. The following devices must be protected with FIPS 140-2 certified encryption:

- All removable storage devices that connect to VA's resources via USB ports (e.g. thumb drives, MP3 Players, external hard drives)
- All devices used to transmit and store VA information outside of VA's protected environment (e.g. laptops, mobile devices)
- Storage media (e.g. CDs, DVDs) that contain VA-sensitive information

If you have any questions about encryption, don't hesitate to ask TS (askTS@va.gov) for assistance or more information.

Check out earlier TS Note editions [here](http://www.techstrategies.oit.va.gov/docs_ctsnotes.asp). (http://www.techstrategies.oit.va.gov/docs_ctsnotes.asp).