nLightenedThoughts

January 2015

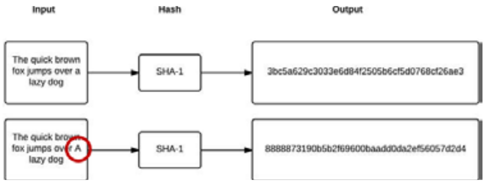
William Blinn Communications
Worthington, Ohio 43085
www.n-lighten.us • 614/859.9359

Encryption Protects Your Information

E-mail is often used to send proprietary information (business development plans, for example) even though most people probably know that e-mail is even less secure than a postcard. Encryption will protect your data, but encryption is puzzling, or frightening, or both.

A vice president of development at CDK Global, Phil Turner, who I've known for more than 30 years, recently explained encryption in an uncommonly clear article that simplifies this complex subject. He gave me permission to use it here.

There are two fundamental tools in modern cryptography: hashes and ciphers. Hashes are used to create a "fingerprint" for a document and only work in one direction. A document is run through a hash algorithm which produces a fingerprint for the document. Every time the document is run through the hash algorithm it produces the same fingerprint, but if anything in the document changes, the fingerprint will change as well.

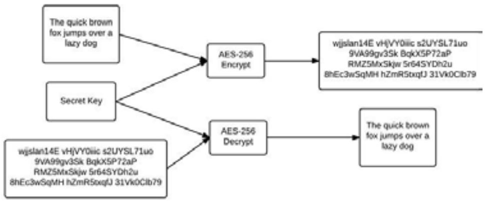

Input
Hash
Output
The quick brown fox jumps over a lazy dog
SHA-1
3bc5a629c3033e6d84f2505b6cf5d0768cf26ae3
The quick brown fox jumps over A lazy dog
SHA-1
8888873190b5b2f69600baadd0da2ef56057d2d4

Ciphers are the workhorse of data encryption and function in two directions: encryption and decryption. A document is run through a cipher's encryption mode and the result is an encrypted document that renders the information in the original document unusable to anyone except the recipient. The encrypted document can then be run through the cipher in decryption mode which then reconstitutes the information in the original document. For the cipher to do its magic, it requires a "key" which is simply a little chunk of data used to uniquely encode the document. How the ciphers use a key separates them into two broad classes: symmetric ciphers and asymmetric ciphers.

Symmetric Ciphers

What makes a cipher symmetric is if the same key is used to both encrypt and decrypt the document.

This key is typically referred to as a "secret key" because anyone with this key can decrypt the encrypted document. One needs to keep the key secret and known only by the originator and intended recipient of the document.

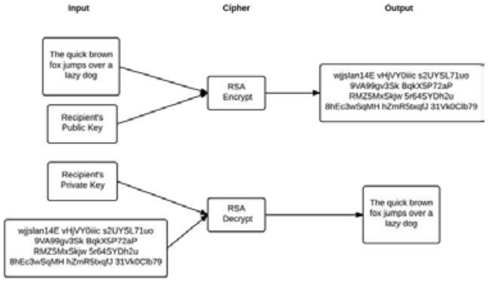

The quick brown fox jumps over a lazy dog
Secret Key
AES-256 Encrypt
wjjslan14E vHjVY0iiic s2UYSL71uo 9VA99gv3Sk BqkX5P72aP RMZ5MxSkjw 5r64SYDh2u 8hEc3wSqMH hZmR5txqfJ 31Vk0Clb79
wjjslan14E vHjVY0iiic s2UYSL71uo 9VA99gv3Sk BqkX5P72aP RMZ5MxSkjw 5r64SYDh2u 8hEc3wSqMH hZmR5txqfJ 31Vk0Clb79
AES-256 Decrypt
The quick brown fox jumps over a lazy dog

The advantages of a symmetric cipher are that it is very fast and there are no restrictions as to the size of the document which can be encrypted with cipher algorithm. The disadvantages of a symmetric cipher are around keeping the secret key known only by the intended recipient. One must choose a "strong" secret key then distribute the key to the recipient in a manner where only the recipient knows the key. The strength of the key is determined by how easy it is to guess the key so creating a long key by randomly selecting numbers, upper, and lower case letters provides a strong key. Selecting short keys or using a single word from the dictionary would create a weak secret key.

Asymmetric Ciphers

A cipher is asymmetric if instead of a single secret key, the cipher uses a pair of keys and whichever key is used to encrypt the data, only the other key in the pair can be used to decrypt the data.

Instead of calling the key a secret key, usually one of the two keys is designated the "private" key and is kept secret, while the other key is designated the "public" key and can be widely distributed without concern about who has access.


Input
Cipher
Output
The quick brown fox jumps over a lazy dog
Recipient's Public Key
RSA Encrypt
wjjslan14E vHjVY0iiic s2UYSL71uo 9VA99gv3Sk BqkX5P72aP RMZ5MxSkjw 5r64SYDh2u 8hEc3wSqMH hZmR5txqfJ 31Vk0Clb79
Recipient's Private Key
wjjslan14E vHjVY0iiic s2UYSL71uo 9VA99gv3Sk BqkX5P72aP RMZ5MxSkjw 5r64SYDh2u 8hEc3wSqMH hZmR5txqfJ 31Vk0Clb79
RSA Decrypt
The quick brown fox jumps over a lazy dog

This allows the recipient to distribute their public key to the originator of a document, and then the originator can encrypt the document with the recipient's public key. The resulting encrypted document can only be decrypted by the recipient with the recipient's private key. This solves the secret key distribution problem, but there are

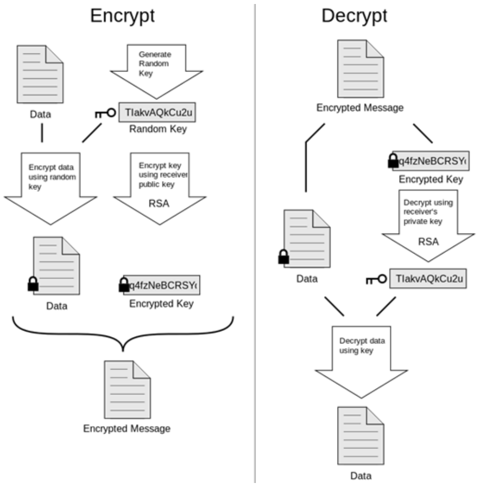
nLightened Thoughts (ISSN 1543-1533) is for clients and friends of n-Lighten.us, 179 Caren Avenue, Worthington, Ohio 43085.
Phone 614.859.9359. On the Web at www.n-Lighten.us. All rights reserved.

two problems with asymmetric ciphers. The first is that they involve very complex computations, so they are slow. The second is that there is a size limitation for the document that can be encrypted by any given key. For example, an asymmetric cipher such as RSA with a 2048-bit key (which is considered to be a long key), can only encrypt around 250 characters of data

PGP – The best of both worlds

PGP encryption leverages both symmetric and asymmetric ciphers to give us the best of both worlds.

When PGP encrypts a document, it generates a long, random, strong one-time-use secret key which is called the session key. This session key is used with a symmetric cipher such as AES-256 to encrypt the document. The session key is then encrypted with an asymmetric cipher such as RSA using the recipient's public key. The encrypted document and the encrypted session key are combined to create the PGP-encrypted message which is sent to the recipient. To decrypt a PGP-encrypted message, the recipient's RSA private key is used to decrypt the session key, then the session key and the AES-256 symmetric cipher is used to decrypt the document.



This allows PGP to solve the key distribution problem using the strengths of an asymmetric cipher and to solve the document length and speed problem using a symmetric cipher. You can find more information for PGP by looking up Pretty Good Privacy (that's what PGP stands for) on Wikipedia.

Digital Signatures – The Extra Credit Problem

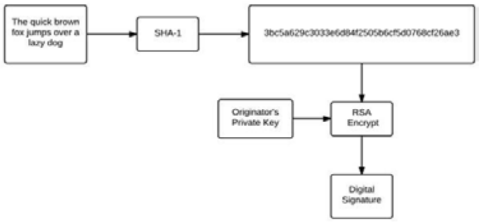
A digital signature allows the recipient of a document to verify that the document was originated from a given party and was not modified in transit. To accomplish this task, we need an asymmetric cipher and the other tool in our cryptography toolbox – the hash.

The process can be simplified by online services that handle encryption and transmission automatically. A Google search for "online encryption" will list numerous options. Encryption should be used whenever you need to send information that should remain private.

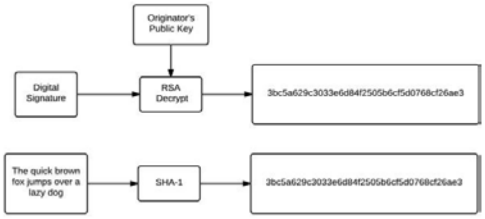
Putting it All Together

First, the originator of the document needs to have an asymmetric cipher key pair and distribute the public key to the intended recipients.

The originator then creates a cryptographic hash of the document, and encrypts that hash using their private key to create the digital signature. The originator can then transmit both the document and the digital signature to the recipient.


The quick brown fox jumps over a lazy dog
SHA-1
3bc5a629c3033e6d84f2505b6cf5d0768cf26ae3
Originator's Private Key
RSA Encrypt
Digital Signature

The recipient, to verify the document, decrypts the hash using the originator's public key and also creates another hash by processing the received document through the hash algorithm. If the two hashes are the same, the document was not altered in transit and was indeed created by the originator.


Originator's Public Key
Digital Signature
RSA Decrypt
3bc5a629c3033e6d84f2505b6cf5d0768cf26ae3
The quick brown fox jumps over a lazy dog
SHA-1
3bc5a629c3033e6d84f2505b6cf5d0768cf26ae3

How do we know this? If the document were modified in transit, the hashes would not match. If the document was forged (created by someone other than the purported originator), then decrypting the encrypted hash with the originator's public key would yield "garbage data" and again, the hashes would not match.

Complicated? Sure, but digital signatures, digital certificates, and SSL are just combinations of these hashes, symmetric, and asymmetric ciphers. Ω