Message digests

Overview

In this section, we will talk about message digests, which take the data in a message and generate a block of bits designed to represent the "fingerprint" of the message.

What is a message digest?

A message digest is a one-way hash function that ensures the integrity of a message. Message digests take a message as input and generate a block of bits, usually several hundred bits long, that represents the fingerprint of the message. A small change in the message creates a noticeable change in the fingerprint. It is a simple matter to generate the fingerprint from the message, but quite difficult to generate a message that matches a given fingerprint.

Algorithms, classes, and methods

JDK supports the following message-digest algorithms:

- MD2 and MD5 , which are 128-bit algorithms
- SHA-1, which is a 160-bit algorithm
- SHA-256,SHA-383, and SHA-512, which offer longer fingerprint sizes of 256, 383, and 512 bits, respectively MD5 and SHA-1 are the most used algorithms.

Example

The MessageDigest class manipulates message digests. The following methods are used in the Message digest code example:

Private key cryptography

Overview

In this section, we'll examine the uses of private key encryption.

What is private key cryptography?

Message digests may ensure integrity of a message, but they can't be used to ensure the confidentiality of a message. For that, we need to use private key cryptography to exchange private messages.
Consider this scenario: Susan and Bob each have a shared key that only they know and they agree to use a same cryptographic algorithm. In other words, they keep their key private. When Susan wants to send a message to Bob, she encrypts the original message, known as plaintext, to create ciphertext and then sends the ciphertext to Bob. Bob receives the ciphertext from Susan and decrypts the ciphertext with his private key to re-create the original plaintext message.

Algorithms, classes, and methods

- DES. DES (Data Encryption Standard) was invented by IBM in the 1970s and adopted by the U.S. government as a standard. It is a 56-bit block cipher.
- AES. AES (Advanced Encryption Standard) replaces DES as the U.S. standard. It was invented by Joan Daemen and Vincent Rijmen and is also known as the Rinjdael algorithm. It is a 128-bit block cipher with key lengths of 128, 192, or 256 bits.

Examples:

Flaw:

But here's the problem: how does the private key get to sender and receiver in the first place? If the sender generates it, he has to send it to the receiver, but it is sensitive information so it should be encrypted. In the next section, we will see how to solve this problem.

Public key cryptography

Overview

In this section, we'll look at public key cryptography, a feature that solves the problem of encrypting messages between parties without prior arrangement on the keys. I will illustrate this with some pictures to make it easier to understand.

- ### Example:

Digital signatures

Did you notice the flaw in the public key message exchange described above? How can Bob prove that the message really came from Susan but not from others? Because anyone who has Bob's public key will be able to encrypt his own message and send the message to Bob, in that Bob will have no way to confirm the message is from Susan. This is known as a Man-in-the-Middle attack. But we can solve this problem by using a digital signature.

In real world, the message digest is signed by the private key. So, if Bob wants to send Susan a signed message, he generates the message digest of the message and signs it with his private key. He sends the message and the signed message digest to Susan. Susan decrypts the signed message digest with Bob's public key and computes the message digest from the cleartext message and checks that the two digests match. If they do, Susan can be sure the message came from Bob.

We'll illustrate an easy way to implement this, by uses the Java language's direct support for signatures.

Note that digital signatures do not provide encryption of the message, so encryption techniques must be used in conjunction with signatures if you also need confidentiality.