CN414
Computer Network Security

Week 6:- Digital Signature

By

Dr. Piya Techateerawat

Digital Signature

- **What is Digital Signature ?**
- Why we need Digital Signature ?
- Digital Signature Application.

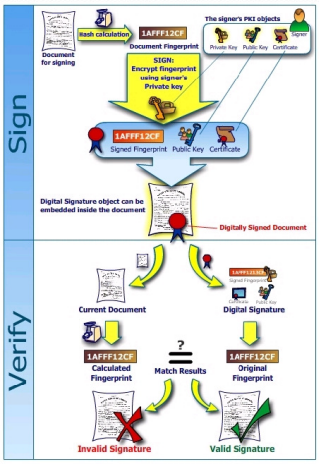
What is Digital Signature?

- A digital signature scheme typically consists of three algorithms:
  - A ***key generation*** algorithm that selects a *private key* uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
  - A ***signing*** algorithm which, given a message and a private key, produces a signature.
  - A ***signature verifying*** algorithm which given a message, public key and a signature, either accepts or rejects.

What is Digital Signature?

- Two main properties are required.
  - First, a signature generated from a fixed message and fixed private key should verify on that message and the corresponding public key.
  - Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

What is Digital Signature?



Digital Signature

- What is Digital Signature ?
- **Why we need Digital Signature ?**
- Digital Signature Application.

Why we need Digital Signature ?

- Authentication
- Integrity

Why we need Digital Signature ?

- Drawback ?

Digital Signature

- What is Digital Signature ?
- Why we need Digital Signature ?
- **Digital Signature Application.**

Digital Signature Application

- Coding in Java

Get a Signature Object:

```
Signature dsa = Signature.getInstance("SHA1withDSA", "SUN");
```

Initialize the Signature Object

```
dsa.initSign(priv);
```

Supply the Signature Object the Data to Be Signed

```
FileInputStream fis = new FileInputStream(args[0]); BufferedInputStream bufin = new
    BufferedInputStream(fis);
byte[] buffer = new byte[1024];
int len;
while (bufin.available() != 0) {
    len = bufin.read(buffer);
    dsa.update(buffer, 0, len);
};
bufin.close();
```

Generate the Signature

```
byte[] realSig = dsa.sign();
```

Reference

- http://java.sun.com/docs/books/tutorial/security/apisign/step3.html

Q & A