Lektion 21

Tirsdag d. 18. april 2023

Læsestof til denne lektion

[Kurose og Ross] 8.1 – 8.4 (dog undtaget afsnittene "Block Ciphers", "Cipher-Block Chaining" og "Why does RSA Work")
(gå generelt let hen over matematikken)

Emner

Netsikkerhed

- Hvor er der trusler?
- Hvad er det vi gerne vil opnå?
- Kryptering
  - Symmetric key
  - Public key
- Beskedsintegritet
- Digital signatur
- CA
- Certifikat
- Autentifikation

Opgaver

Opgave 27
Workshop i kryptering

Læsestof til næste lektion

[Kurose og Ross] 8.6 og 8.9

Bemærkninger:

Opgave 27

Denne opgave handler om at analysere en mulig algoritme til symmetric (secret) key kryptering.

Funktionerne til kryptering og dekryptering er vist herunder:

```
public static String krypt(String s,int key) {
            StringBuffer temp = new StringBuffer();
            for (int i = 0; i < s.length();i++)
              temp.append((char)(((int)(s.charAt(i))+key)%256));
            return temp.toString();
}

public static String dekrypt(String s,int key) {
            StringBuffer temp = new StringBuffer();
            for (int i = 0; i < s.length();i++)
              temp.append((char)(((int)(s.charAt(i))-key)%256));
            return temp.toString();
}
```

Hvordan krypterer denne metode ?

Hvilke ulemper har denne metode ?

Kunne du foreslå forbedringer til metoderne ?

Ovennævnte viser princippet i en krypteringsfunktion, men der er faktisk en programmeringsfejl i ovenstående – har du fundet den?

Workshop Security

Public Key encryption using GPG

GPG stands for Gnu Privacy Guard (and works much the same as PGP, Pretty Good Privacy). You can download it for Windows from http://gpg4win.org/ - take the full version. Mac users should go to http://www.gpgtools.org/ and Linux users should use their package management.

Under Choose Components select only GnuPG and Kleopatra.

What you get is a GUI-app called Kleopatra (...silly name...).

Exercise 1

The first thing to do is to generate your own pair of private/public keys.

Run Kleopatra, choose File | New OpenPgP Key Pair and make a personal OpenPGP-Key Pair.

Give it your own firstname as name.

Enter a passphrase with at least 10 characters and remember the passphrase.

Press Afslut

Right-click the certificate you just made and export it to a file on your desktop. Give the file your own firstname as filename. The file now contains your public key.

Upload the file to Discord

Exercise 2

You are now ready to start the encrypted communication.

Find a body to whom you want to send a secret message. On Discord find the public key file belonging to the body and copy it to your desktop.

Import the public key into Kleopatra.

Make a small file with a “secret” text (use NotePad).

Choose Signer/Krypter to enkrypt your secret tekst.

Use NotePad to look at the file and see it is encrypted

Place the encrypted file on Discord (with filename *TOyourbodyname* and let your body pick the file and decrypt it.

Exercise 3

Is there any problems left in the scenario you just saw.