Kryptovanie a podpisovanie

Pri komunikácii v nechránenom potenciálne nebezpečnom prostredí je možné:

1. zabezpečiť, aby sme o správach, ktoré získame z určitého zdroja vedeli povedať, či naozaj z tohto zdroja pochádzajú (t.j. nikto nemôže po ceste správu zmeniť, alebo pridať)
 => podpisovanie (sign – verify)

2. zabezpečiť, aby nám bolo možné poslať správu kryptovane a nikto, okrem odosielateľa si ju nemohol po ceste prečítať
 => kryptovanie (encrypt – decrypt)

Podpisovanie - ako to funguje?

Odosielateľovi, ktorého identitu správ budeme chieť zaručiť, vygenerujeme dvojicu kľúčov (private – public). Private key ostane iba u odosielateľa. Pomocou private key vypočíta ku každej svojej správe podpis a tento podpis pribalí ku správe.

Všetkým potenciálnym adresátom správy dá k dispozícii public key, pomocou ktorého vedia overiť, či podpis patrí k doručenej správe.

Kryptovanie – ako to funguje?

Adresát, ktorý chce prijímať kryptované správy si vygeneruje dvojicu kľúčov (public – private). Všetkým potenciálnym odosielateľom zverejní svoj public key. Tí pomocou neho zakódujú každú správu tak, že ju nevie rozkódovať nikto iný, ako ten, čo má private key – ten však zostáva iba u chráneného adresáta. Iba adresát pomocou svojho private key dokáže dekódovať zakódovanú správu.

Podpisovanie a kryptovanie môžeme kombinovať, ak chceme zaručiť, že správa pochádza z overeného zdroja a nikto ju po ceste nemohol prečítať.

Podpisovanie a kryptovanie v Jave

Súčasťou API – na podpisovanie stačí
```
import java.security.*;
```

na kryptovanie treba:
```
import javax.crypto.Cipher;
```

najskôr treba vždy vygenerovať pár prislúchajúcich kľúčov:

```
KeyPair key = KeyPairGenerator.getInstance("RSA")
                    .generateKeyPair();
```

private a public key môžeme serializáciou zapisovať do / čítať zo súboru:

```
key.getPrivate(), key.getPublic()
```

Podpisovanie v Jave

Podpísanie:

```
Signature podpis = Signature.getInstance("SHA1withRSA");
podpis.initSign(privateKey);
podpis.update(message);
return podpis.sign();
```

Kontrola:

```
Signature podpis = Signature.getInstance("SHA1withRSA");
podpis.initVerify(publicKey);
podpis.update(message);
return podpis.verify(p);
```

Kryptovanie v Jave

Zakódovanie:

```
Cipher crypto = Cipher.getInstance("RSA");
crypto.init(Cipher.ENCRYPT_MODE, publicKey);
return crypto.doFinal(s.getBytes());
```

Odkódovanie:

```
Cipher crypto = Cipher.getInstance("RSA");
crypto.init(Cipher.DECRYPT_MODE, privateKey);
return new String(crypto.doFinal(s));
```