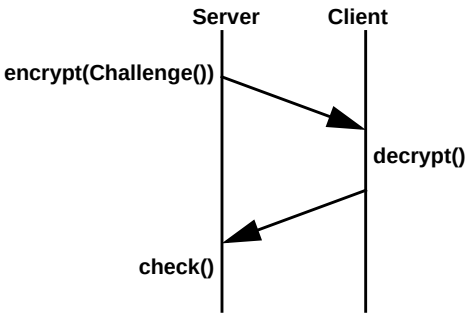
Übungsaufgabe #3: Challenge-Response

3.12.2008

In dieser Aufgabe soll eine Challenge-Response-Authentifizierung mit öffentlichen und privaten Schlüsseln implementiert werden.



Hierbei soll eine auf dem Server generierte zufällige Challenge (auch Nonce genannt) mit dem öffentlichen Schlüssel des Clients verschlüsselt, Base64 enkodiert und ausgegeben werden. Anschliessend soll der Server auf die Eingabe der entschlüsselten (Base64 enkodierten) Challenge warten und diese überprüfen.

Der Client soll zur Eingabe des Passworts des privaten Schlüssels auffordern und danach auf die Eingabe der Base64 enkodierte Challenge warten. Diese soll mit seinem privaten Schlüssel entschlüsselt und Base64 enkodiert ausgegeben werden. Der private Schlüssel kann fest in den Client gelinkt oder aus einer Datei gelesen werden.

Schlüssel generieren:

```
$ openssl genrsa -out privkey.pem -aes256 1024
$ openssl rsa -in privkey.pem -pubout -out pubkey.pem
```

Schlüssel linken (Zugriff über `extern char _binary_privkey_pem_start[];`):

```
$ ld -r -b binary -o privkey.o privkey.pem
$ objcopy --rename-section .data=.rodata,alloc,load,readonly,data,contents
  privkey.o privkey.o
```

Server:

```
$ ./server pubkey.pem
Please challenge the following BASE64 string:
erq...btA=
Enter your response and press Ctrl-D when finished:
ZWg...8Ug=
Done reading input.
Challenge successful, proceeding ...
```

Client:

```
$ ./client
Enter PEM pass phrase:
Enter the challenge, when finished, press Ctrl-D:
erq...btA=
Done reading input.
The Response is:
ZWg...8Ug=
```

Parameter:
Es sollen RSA-AES256 Schlüssel mit einer Länge von 1024 Bit verwendet werden. Die Challenge sollte die gleiche Länge wie der genutzte Schlüssel haben und kann mit `RSA_size(pubkey) - 42` berechnet werden.
Die Abgabe der bearbeiteten Aufgabe erfolgt spätestens in den Übungen am 17. oder 19.12. Eine vorzeitige Abgabe ist möglich und ausdrücklich erwünscht! Die Bearbeitung kann in Gruppen zu zwei oder drei Personen erfolgen.