Amir Azodi (amir.azodi@hpi.uni-potsdam.de)
Marian Gawron (marian.gawron@hpi.uni-potsdam.de)
Dr. Feng Cheng, (feng.cheng@hpi.uni-potsdam.de)

November 13th, 2013 (Hand-In November 27th, 2013)

Exercise #3
Internet Security – Weaknesses and Targets
Prof. Dr. Ch. Meinel
Winter 2013/14

Topic: Cryptography
Maximum points: 110%

tasks

1. Explain the term Hybrid Encryption.
   Hints: *Where do we use Hybrid Encryption to protect Data? What is the reason to use Hybrid Encryption?* 15%

2. Implement (using Python or Java) the RSA algorithm. The application should take three commands: 25%
   key-gen: your app should generate two prime numbers (p, q) in the range of (100 - 5000) and use them to generate a private and a public key.
   The *key-gen* should **check for existing prime numbers first**. If they exist use this numbers to generate the keys, if not create the prime numbers
   encrypt "plaintext": your app should take the text (in between the quotation marks), encrypt it using your public key and print (only) the ciphertext.
   decrypt "ciphertext": your app should take the ciphertext (in between the quotation marks), decrypt it using your private key and print the resulting plaintext.

   Prime numbers should be generated freshly every time the key-gen command is executed and they should be stored inside a text file. The encrypt and decrypt commands should read the text file, if existing, and invoke the key-gen command otherwise.

   Contents of the text file (./crypto.conf)=
   ```
   prime1
   prime2
   public key
   private key
   ```
   (this text-file will be replaced by the correctors to test application functionality).

3. Explain the concept of "padding" in RSA. 20%

4. Describe the idea of Forward Secrecy. What is the goal/advantage of Forward Secrecy? Which kinds of attacks are still possible? Give an example how to achieve Forward Secrecy. 15%

5. In group theory: What are the characteristics of an Abelian Group? Why do we use cyclic groups (e.g. in Diffie-Hellman) ? 20%

6. Explain the difference between ECB, CBC, CFB, and OFB modes in block ciphers. What are the benefits of each modus? What are the security implications of a published initialization vector? 15%

Hand-in: November 27th, 2013, 12:00 p.m. online at `fb10moodle.hpi.uni-potsdam.de`
File format: **firstname-lastname_03.zip**