1. **RSA-Padding and CCA-Security**: Exercise 10.14 in [KL]. **Hint**: Use messages $m_0, m_1$ whose ciphertexts you can transform into different valid ciphertexts if the most significant bit of the random part $r$ of the padding is 0.

![Image](wikimedia.org)

left: The $\text{PubK}_{\mathcal{A},\Pi}^\text{cca}(n)$ experiment, right: Optimal Asymmetric Encryption Padding (OAEP)

2. **El Gamal Variant**: Exercise 10.11 in [KL].

3. **Secure Coin-Flipping**: Exercise 10.17 in [KL].

4. **Paillier Encryption**:
   (a) Exercise 11.16 in [KL].
   (b) Exercise 11.15 in [KL].
   (c) Show that the hardness of the decisional residuosity problem with respect to $\text{GenModulus}$ (as in Definition 11.31) implies the hardness of factoring with respect to $\text{GenModulus}$ (as in Definition 7.45). **Hint**: use (b).

5. **(In-)Security of Textbook RSA Signatures for Weaker Security Notions**: Exercise 12.2 in [KL].

6. **Encoded RSA**: Exercise 12.4 in [KL].

7. **Public-Key Infrastructures**: Exercise 12.13 in [KL]
8. **Secure E-mail in Practice:** (This is a *bonus* exercise!) Send and receive PGP-encrypted e-mail. Start from [http://www.gnupg.org/](http://www.gnupg.org/) (GnuPG, includes links to Windows/Mac OS), look at [http://enigmail.mozdev.org/documentation/quickstart.php.html](http://enigmail.mozdev.org/documentation/quickstart.php.html) (Thunderbird), or use whatever software makes sense for you.

(a) There are several files in [http://homepages.cwi.nl/~schaffne/course/pgp/](http://homepages.cwi.nl/~schaffne/course/pgp/). What can you tell us about these files?

(b) Send an e-mail, encrypted and signed by your personal key, to both Maria and Christian. Ideally, your public key should be on the public keyservers; if you don’t want to upload it, please send it to us (in the same or a separate message).