6. Assignment
Introduction to modern Cryptography
(Summer Term 2019)

Bauhaus-Universität Weimar, Chair of Media Security (Prof. Lucks)
Teacher: Nathalie Dittrich
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`
Submission: 02.07.2019, 03:15 PM before the start of the lab class via moodle (preferred) or analogue on paper.
LaTeX-Template: template.tex

Task 1 – Block-Cipher Modes (4 Points)
Alice wants to send the two-block (32 characters) message

$$M = (M_1, M_2) = \texttt{Send␣to␣Bob␣100,-␣EUR␣from␣Alice}$$

with $M_1, M_2 \in \{0,1\}^n$ encoded as 8-bit ASCII string encrypted to her bank. Alice chooses an initial value $IV \in \{0,1\}^n$, encrypts M with AES-128 in some mode and her secret key, and transmits the resulting ciphertext (IV, C_1, C_2) to her bank.
An adversary Eve intercepts Alice's ciphertext. Instead of the original text, Eve wants to replace it with a manipulated ciphertext $C' = (IV',\, C_1',\, C_2')$ for the message

$$M' = (M_1', M_2') = \texttt{Send␣to␣Eve␣500,-␣EUR␣from␣Alice}$$

a) Specify a possible ciphertext (IV', C_1', C_2') for M' when the used mode is Counter mode.

b) Specify a possible ciphertext (IV', C_1', C_2') for M' when the used mode is CBC.

Hint: Note that Eve can freely choose a new initial value IV'.

Task 2 – Homomorphic Encryption (3 Points)
RSA (and ElGamal and Diffie-Hellman) are a homomorphic cryptosystem because we can change the output in a way such that we can predict how the input will change.

a) Let $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_n$. Find a homomorphism (this means operations $\circ$ and $\bullet$) for a (naive) signaturefunction of RSA: $F(m) := m^d \bmod n$.

b) Please explain: Does this property make (naive) RSA signatures more secure or less? If it makes it more secure, give one example of a simple attack on naive RSA signatures that could be prevented thanks to this property. Otherwise give an example for a possible attack.

Task 3 – Hybrid Encryption (4+2 Points)
Alice and Bob want to use a hybrid encryption system. Alice chooses a 64-bit key K and encrypts it with Bob's public RSA key (n, e) to $Y \leftarrow (0 \dots 0 \,\|\, K)^e \bmod n$. Afterwards she encrypts her message M to $C \leftarrow E_K(M)$ with a symmetric cipher E and sends (Y, C) to Bob. Bob first computes $K' = Y^d \bmod n$ and then decrypts $M = E_{K'}^{-1}(C)$. Eve eavesdrops (Y, C) and wants to obtain K.

a) Assume Bob tests if it holds that $K' < 2^{64}$ and if $K' \geq 2^{64}$ he outputs an error message. Describe an efficient algorithm which Bob could use as an oracle, this means he formulares requests (Y', C) and in the end he can derive Alice's K with significant probability. (*Hint:* Read chapter 3-5 from [1]).

b) What should Bob do instead if he notices that K' is invalid?

Task 4 – ECB vs. CBC (Bachelor: +4 Points, Master: 4 Points)
Write a python program that encrypts the given image `cat.bmp` with AES. Encrypt it once in combination with ECB and once with CBC.
Your program should take as arguments the input- and output file and the desired mode. A program call could look as follows:

```
python3 image_encryption_123456.py -i cat.tiff -o cat_enc.tiff -m ECB
```

Compare the two output images. What do you see? Explain your findings.
You don't have to submit the generated images. It is sufficient to submit the working code and the explanation stated above. You don't have to implement AES or the given modes by yourself. Use a good crypto-library instead.

Literatur

[1] Kühn, Ulrich. "Side-channel attacks on textbook RSA and ElGamal encryption." Public Key Cryptography—PKC 2003. Springer Berlin Heidelberg, 2002. 324-336.