Problem Set 1
Introduction to Modern Cryptography
Online Course (Winter Term 2018)

Bauhaus-Universität Weimar, Chair of Media Security
Course: Prof Dan Boneh, Stanford University, Problem Session: Nathalie Dittrich.
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`
Due Date: 25 November, 11:59 PM, via email to
`nathalie.jolanthe.dittrich(at)uni-weimar.de`.
Note: For all tasks, explain your solutions in brief in your own words. The use of LaTeX is recommended; a LaTeX template file can be found on the website of the problem session.

Question 1 – PRGs (6 Points)
Let $G : \{0,1\}^k \rightarrow \{0,1\}^n$ be a secure pseudo-random generator (PRG) which takes a k-bit seed K and outputs an n-bit pseudorandom value. Which of the following are also secure PRGs? Briefly explain your answers.

- ☐ $G'(K) := \text{reverse}(G(K))$ (reverse(X) inverts the bit order of X)
- ☐ $G'(K) := G(0^k)$
- ☐ $G'(K) := G(K) \oplus G(0^k)$
- ☐ $G'(K, K') := G(K) \wedge G(K')$, where K and K' are independent uniformly at random chosen k-bit seeds
- ☐ $G'(K) := G(K) \,\|\, G(K)$ ($\|$ denotes concatenation)
- ☐ $G'(K) := G(K) \oplus 1^n$ (1^n denotes an n-bit string 11111..).

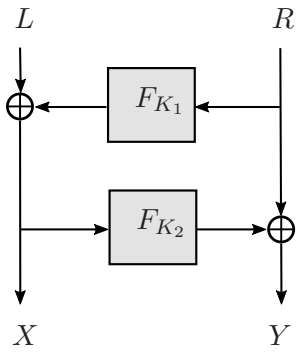
Question 2 – Two-Time Pad (4 Points)
Alice manages a renowned football club. Yesterday, she heard that an opponent club wants to buy one of her best players. She is told that her employees intercepted the message "`Engage␣Neymar`" which was One-Time-Pad encrypted to

`0xccc57a7c2ed8b1c4e506d17957`

from the other club (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hexadecimal). To confuse the opponent club, Alice would like to manipulate the message and send the manipulated message instead. Calculate the One-Time-Pad encryption of the message "`Engage␣Suarez`" under the same key, and explain your solution.

Question 3 – Feistel (4 Points)
Let $E : \{0,1\}^{2k} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ be a **two-round** Feistel network that uses a secure pseudo-random function (PRF) $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ with a first key K_1 in the first, and an independent secret key K_2 in the second round. Both keys are secret and were chosen uniformly at random from $\{0,1\}^k$. A $2n$-bit plaintext $M = (L, R)$ is encrypted to a $2n$-bit ciphertext (X, Y) as illustrated below.

Let $\mathcal{A}$ be an adversary with access to an oracle O to which $\mathcal{A}$ asks queries. At the beginning, O chooses independent secret keys K_1 and K_2 uniformly at random, and tosses a fair coin to obtain a bit $b \in \{0,1\}$. For each query, $\mathcal{A}$ must provide two $2n$-bit messages $(L_0, R_0), (L_1, R_1)$. O responds with $E_{K_1,K_2}(L_b, R_b)$. $\mathcal{A}$ is not allowed to ask the same message twice to the oracle. Describe an attack on the two-round Feistel cipher with at most two queries. Specify the advantage of your attack.



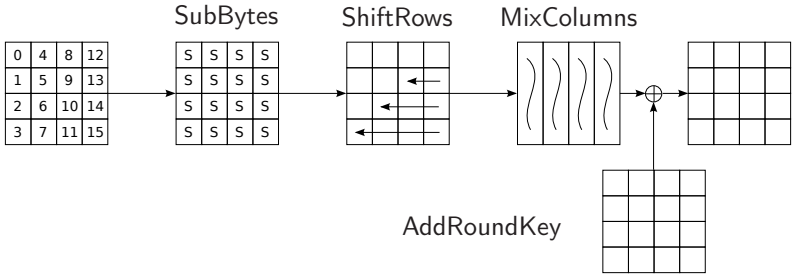
Question 4 – 4DES Encryption (4 Points)
Since the DES uses only 56-bit keys, Alice wants to construct a cipher with higher security. She defines $4DES : \{0,1\}^{56} \times \{0,1\}^{56} \times \{0,1\}^n \to \{0,1\}^n$, which uses a 112-bit key, consisting of two independent secret 56-bit keys K_1 and K_2, and four calls of the original DES:

$$4DES_{K_1,K_2}(M) = DES_{K_2}(DES_{K_2}(DES_{K_1}(DES_{K_1}(M)))).$$

a) Describe a key-recovery attack on $4DES$ that takes significantly less time than testing all 2^{112} keys. Specify your attack time and memory complexities.

b) Describe (briefly) how one could modify 4DES such that the attack from a) are made infeasible.

Question 5 – AES (4 Points)
The AES has 10 rounds where each of its 10 rounds consists of SubBytes, ShiftRows, MixColumns and AddRoundKey (except for the last round). The figure below shows one round of AES. The input on the left also shows the order of the bytes in the state.



Let $P, P' \in \{0,1\}^{128}$ be two plaintexts differening only in Byte 0 (encoded in hexadecimal):

$$P = \texttt{0x0001020304050607 08090a0b0c0d0e0f},$$
$$P' = \texttt{0xff01020304050607 08090a0b0c0d0e0f}.$$

Both plaintexts are encrypted with three different modified versions of the AES:

1. An AES version where MixColumns is omitted in every round.
2. An AES version where ShiftRows is omitted in every round.
3. A complete AES version.

Below, you find three ciphertext pairs, encoded in hexadecimal. For all pairs, C_i is the ciphertext of P and C_i' that of P'. Briefly explain which ciphertext pair (C_i, C_i') is generated by which modified version of AES from above.

$C_1 = \texttt{0x231446982181c5ca6476f957632cbd2a}$, $C_1' = \texttt{0xbbac089c1cc8ff7e83f147177b488316}$

$C_2 = \texttt{0xceee58e94372694000fc7e2466b25564c}$, $C_2' = \texttt{0xb7ee58e94372694000fc7e2466b25564c}$

$C_3 = \texttt{0x2b45b04bce63e0c1e750ca0c876248a9}$, $C_3' = \texttt{0xb6012b6ece63e0c1e750ca0c876248a9}$

Question 6 – 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'.

Question 7 – Simple MACs (4 Points)
For each of the following MACs, briefly explain why they are secure or show how to efficiently forge the authentication code for a message. Prior, you can ask for the authentication of up to three chosen messages.

a) $MAC_K(M) := \bigoplus_{i=1}^{m} E_K(M_i)$.

b) $MAC_K(M) := \bigoplus_{i=1}^{m} E_{K \oplus \langle i \rangle}(M_i)$.

c) $MAC_K(M) := \bigoplus_{i=1}^{m} E_K(M_i \oplus \langle i \rangle)$, where $\langle i \rangle$ denotes the n-bit representation of i.

Question 8 – CBC-MAC' (4 Points)
Assume that $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a secure block cipher and $K_1 \in \{0,1\}^k$ a secret key. Let $K_2 \in \{0,1\}^n$ be a second independent key. We consider the following variant of CBC-MAC, called CBC-MAC'. Given an m-block message $M = (M_1, \ldots, M_m)$, CBC-MAC' computes an authentication tag as follows:

$$\begin{aligned} C_0 &= 0^n, \\ C_i &= E_{K_1}(C_{i-1} \oplus M_i), \qquad \text{for } 1 \le i \le m, \\ \text{CBC-MAC}'_{K_1,K_2}(M) &:= C_m \oplus K_2, \end{aligned}$$

Show how to efficiently predict the tag for a message with CBC-MAC'. You may ask for the tags of at most three (other) messages before. Note that you can vary the lengths of your chosen messages.