2. Problem Session
Introduction to Modern Cryptography
(Online Course (Winter Semester 2016/17)

Bauhaus-Universität Weimar, Professur für Mediensicherheit
Course: Prof Dan Boneh, Stanford University, Problem Session: Farzaneh Abed.
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`

Date: Monday: 28.11.2016 (15:15)

Question 1 – DES S-boxes (2 Points)
S-boxes are the only non-linear functions in DES. By this task, you need to prove this property by computing the output of S_8 for several pairs of inputs. Show that $S_8(x_1) \oplus S_8(x_2) \neq S_8(x_1 \oplus x_2)$ for the following x_1 and x_2:

1. $x_1 = 000100, x_2 = 001001$
2. $x_1 = 000000, x_2 = 100001$
3. $x_1 = 101010, x_2 = 010101$

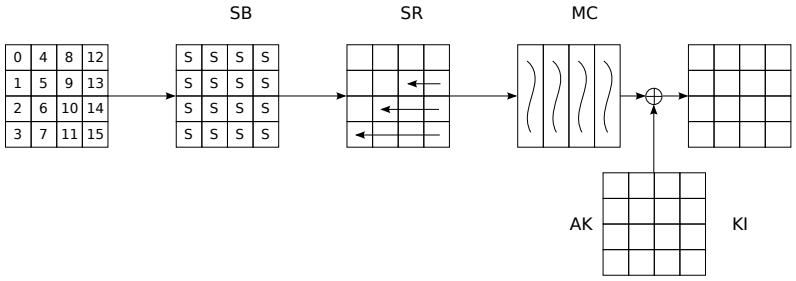
Question 2 – DES Block Cipher (1 Points)

1. What is the key and block size of DES?
2. How many S-boxes DES has? What's the input and output size?
3. What are the components of DES block cipher?
4. Which component provides confusion and which one diffusion?

Question 3 – AES Block Cipher (1 Points)

1. What is the key and block size, and number of rounds for AES?
2. What is the component of AES block cipher?
3. Which component provides confusion and which one diffusion?
4. Which property the transformation matrix should have to be able to decrypt any message?

Question 4 – AES (4 Points)
The AES-128 is the block cipher with 10 rounds, each consists of SubBytes, ShiftRows, MixColumns and AddRoundKey (except for the last round). The figure shows the one round of AES, where the input on the left shows the order of the bytes in the state.



Let $M, M' \in \{0,1\}^{128}$ be two plaintexts that differ only in byte 0 (here encoded in hexadecimal):

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

Both messages are encrypted with three different versions of AES as follows:

1. An AES without a MixColumns in every round.
2. An AES without a ShiftRows in every round.
3. A complete AES.

For the following ciphertext pairs $(C_i, C'i)$ which is the encryption of (M, M'), find out which ciphertext pair is generated by which version of the AES mentioned above, and briefly explain your choice.

$C_1 = \texttt{0x231446982181c5ca 6476f957632cbd2a}$, $C'_1 = \texttt{0xbbac089c1cc8ff7e 83f147177b488316}$
$C_2 = \texttt{0xceee58e943726940 0fc7e2466b25564c}$, $C'_2 = \texttt{0xb7ee58e943726940 0fc7e2466b25564c}$
$C_3 = \texttt{0x2b45b04bce63e0c1 e750ca0c876248a9}$, $C'_3 = \texttt{0xb6012b6ece63e0c1 e750ca0c876248a9}$

Question 5 – Mode of Operation (4 Points)
Bob wants to send the two-block (32 characters) message

$$M = (M_1, M_2) = \texttt{Send␣to␣Feri␣100,␣Euro␣from␣Bob}$$

with $M_1, M_2 \in \{0,1\}^n$ encoded as 8-bit ASCII string encrypted to his bank. Bob chooses an initial value $IV \in \{0,1\}^n$, encrypts M with AES-128 in some mode and his secret key, and transmits the resulting ciphertext (IV, C_1, C_2) to his bank.
An adversary Eve intercepts Bob'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

$$M' = (M'_1, M'_2) = \texttt{Send␣to␣Eve␣1000,␣Euro␣from␣Bob}$$

a) What is the possible ciphertext (IV', C_1', C_2') for M' when you use Counter mode.

b) What is the ciphertext (IV', C_1', C_2') for M' when you use CBC mode.

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

Question 6 – OFB Mode (4 Points)
Assume that I have sent you an encrypted message by using DES in OFB mode of operation with a fixed secret key IV.

1. Explain a known-plaintext attack that helps you to decrypt the message.
2. How about CBC and CFB modes? Are they stronger? Explain your answer.

Question 7 – Simplified DES (4 Points)
Let $K_1, K_2, \ldots, K_{16}$ be a random element in $\{0,1\}^{32}$. We simplify round function of DES, $f_1, \ldots, f_{16} : \{0,1\}^{32} \to \{0,1\}^{32}$, and define it as

$$f_i(x) = x \oplus K_i.$$

The key for the simplified DES is then $K' = (K_1, \ldots, K_{16})$ with the size of $16 \times 32 = 512$ bits. Is the resulting cipher breakable? Explain why. Precisely, suppose you given a few plaintext/ciphertext pairs $(m_i, E(K', m_i))$ for $i = 1, 2, \ldots, 10$, the m_i is chosen randomly from $\{0,1\}^{64}$. Show how to use this data to decrypt any ciphertext, i.e, by given $E(K', m)$, how to recover m.