Cryptography, winter 2006

PROF. DR. WERNER SCHINDLER, DIPL.-INF. DANIEL LOEBENBERGER

3. Exercise sheet (22.11.2006)
Hand in solutions to the homework exercises on Wednesday, December 6th, in the tutorial/the lecture.

Exercise 3.1 (Repetition: Elementary stochastics).

On a conference on Internet security are 15% *of the people cryptographers.* 90% *of the cryptographers drink coffee. In total* 25% *of the participants of the conference drink coffee. In the morning you see a person drinking coffee. What is the probability that this person is a cryptographer?*

Solution. Let A be the event "A (uniformly) selected person is cryptographer" and B the event "A (uniformly) selected person drinks coffee". We know $\text{prob}\,(A) = 0.15$ and $\text{prob}\,(B) = 0.25$. It is given that $\text{prob}\,(B|A) = 0.9$. We want to know $\text{prob}\,(A|B)$. By Bayes theorem we have

$$\text{prob}\,(A|B) = \frac{\text{prob}\,(B|A) \cdot \text{prob}\,(A)}{\text{prob}\,(B)}$$

Thus we have $\text{prob}\,(A|B) = \frac{0.9 \cdot 0.15}{0.25} = 0.54$. ◯

Exercise 3.2 (Modes of Operation).

Recall that S_n *is the set of all bit permutations of the set* $\{0,1\}^n$*. Let* $\pi \in S_n$*. Consider the following block cipher*

$$\eta_\pi \colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n, (x_0, \ldots, x_{n-1}) \mapsto (x_{\pi(0)}, \ldots, x_{\pi(n-1)})$$

Decrypt the ciphertext `101010101010` *using ECB mode, CBC mode and OFB mode. Use the cipher defined above with block length* 3 *and key*

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

The initialization vector is 000*. For the OFB mode, use* $r = 2$*.*

Solution. ECB: `011100011100`, CBC: `011001001001`, OFB: `101010101010` ◯

Exercise 3.3 (Perfect secrecy: The Two Time Pad).

Show that the one-time pad is no longer unconditionally secure (perfect secrecy) if a key is used two (or more) times.

Solution. Let $m_1, m_2 \in \{0,1\}^n$ be two messages of length n, and let $k \in \{0,1\}^n$ be the key. Assume you observe two ciphertexts $c_1, c_2 \in \{0,1\}^n$ with $c_i := m_i \oplus k$ for $i \in \{1,2\}$. Then

$$c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

Thus the observation of c_1 and c_2 leaks information on m_1 and m_2. ◯

Exercise 3.4 (Homework: Forging the IV). (7 points)

7

Consider the following ASCII table

Binary	Decimal	Hexadecimal	Glyph
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z

Assume you intercepted a message (m, IV), $m \in \{0,1\}^*, \text{IV} \in \{0,1\}^{64}$ where the plaintext was encoded according to the above ASCII table and encrypted with the CBC mode of a block cipher with block length 64 bit and initialization vector IV=`0xAAAAAAAAAAAAAAAA` yielding m. Assume further you know that the plaintext of the message starts with the phrase `DEAR SIR`. Find an initialization vector IV′ such that the decrypted message will start with `DEAR MAM`.

Solution.
MAM = 4D 41 4D = 01001101 01000001 01001101
SIR = 53 49 52 = 01010011 01001001 01010010

The modified initialization vector is

$$IV = \texttt{0xAAAAAAAAAAAAB4A2B4}$$

◯

Exercise 3.5 (Homework: Perfect Secrecy). (5 points)

Prove that the Caesar cipher is not unconditionally secure. 5

Solution. We consider a pair of ciphertext letters $(c_1, c_2) \in \mathbb{Z}_{26}^2$. The probability for a plaintext pair $(p_1, p_2) \in \mathbb{Z}_{26}^2$ with $c_1 - c_2 \neq p_1 - p_2 \pmod{26}$ is zero, the probability for a plaintext pair $(p_1, p_2) \in \mathbb{Z}_{26}^2$ with $c_1 - c_2 = p_1 - p_2 \pmod{26}$ is $1/26$. Thus the Caesar cipher is not unconditionally secure, whenever the plaintext has more than one letter. Otherwise we have perfect secrecy. ◯

Exercise 3.6 (Homework: Modes of Operation). (8 points)

Decrypt the ciphertext `111111111111` using ECB mode and CBC mode. Use the cipher defined in Exercise 3.2 with block length 3 and key 8

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Solution. ECB: `111111111111`, CBC: `111000000000` ◯