Cryptography, winter 2006

Prof. Dr. Werner Schindler, Dipl.-Inf. Daniel Loebenberger

4. Exercise sheet (29.11.2006)
Hand in solutions to the homework exercises
on Wednesday, December 20th, in the tutorial/the lecture.

Exercise 4.1 (Repetition: Power of 3).

Compute $3^{1\,000\,003} \bmod 101$ *by hand.* Note*: Only a small calculation is needed!*

Solution. We have $\varphi(101) = 100$ since 101 is prime. By Euler's theorem we have $a^{\varphi(n)} \equiv 1 \pmod{n}$ for all $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Thus

$$3^{1\,000\,003} \equiv 3^{1\,000\,003 \bmod \varphi(101)} \equiv 3^3 \equiv 27 \pmod{101}$$

○

Exercise 4.2 (Perfect secrecy).

In this exercise we study the impact of non-uniform key selection.

For this purpose consider the encryption system $y = e_k(x)$ *when* e *is the encryption function,* k *is the encryption key, that can belong to a set* $K = \{1, 2, 3, 4\}$*. The plain text* x *and the cipher text* y *belong both to same set* $P = C = \{a, b, c, d\}$*. We express mapping rule with a table as follows:*

	a	b	c	d
1	b	c	d	a
2	c	d	a	b
3	d	a	b	c
4	a	b	c	d

This means, for instance, that key 1 maps the character a to b while key 4 induces the identity mapping.

Suppose that the character a *appears as plain text with probability* $1/2$*, that is* $\text{prob}(\mathcal{P} = a) = 1/2$*. Suppose further that* $\text{prob}(\mathcal{P} = b) = 1/4$*,* $\text{prob}(\mathcal{P} = c) = 1/8$*,* $\text{prob}(\mathcal{P} = d) = 1/8$*. The key is selected independently from the plaintext.*

(i) *Show the identity*

$$\text{prob}(\mathcal{C} = y) = \sum_{x, e_k(x) = y} \text{prob}(\mathcal{P} = x) \cdot \text{prob}(\mathcal{K} = k).$$

Solution. We have

$$\sum_{x,e_k(x)=y} \operatorname{prob}(\mathcal{P}=x)\cdot\operatorname{prob}(\mathcal{K}=k) = \sum_{x,e_k(x)=y} \operatorname{prob}(\mathcal{P}=x \wedge \mathcal{K}=k)$$

by statistical independence. Since the events are disjunct we obtain

$$\begin{aligned}\sum_{x,e_k(x)=y} \operatorname{prob}(\mathcal{P}=x \wedge \mathcal{K}=k) &= \operatorname{prob}\left(\biguplus_{x,e_k(x)=y} (\mathcal{P}=x \wedge \mathcal{K}=k)\right)\\ &= \operatorname{prob}(\mathcal{C}=y)\end{aligned}$$

$\bigcirc$

(ii) Suppose $\operatorname{prob}(\mathcal{K}=1)=1/3$, $\operatorname{prob}(\mathcal{K}=2)=1/3$, $\operatorname{prob}(\mathcal{K}=3)=1/3$, $\operatorname{prob}(\mathcal{K}=4)=0$.

(a) For each of characters a, b, c, d compute probability of observing them as output.

Solution.

$\mathcal{C}$	a	b	c	d
$\operatorname{prob}(\mathcal{C}=y)$	1/6	1/4	7/24	7/24

$\bigcirc$

(b) Compute conditional probability $\operatorname{prob}\,(\mathcal{P}=x\,|\,\mathcal{C}=y)$ *that the plain text was x if we observe the cipher text y for each $x \in \{a,b,c,d\}$, $y \in \{a,b,c,d\}$.*

Solution. We have $\operatorname{prob}(\mathcal{C}=y;\mathcal{P}=x) = \sum_{k,x=d_k(y)} \operatorname{prob}(\mathcal{K}=k)$. Thus by the Bayesian theorem

$$\operatorname{prob}\,(\mathcal{P}=x\,|\,\mathcal{C}=y) = \frac{\operatorname{prob}(\mathcal{P}=x)\cdot\sum_{k,x=d_k(y)}\operatorname{prob}(\mathcal{K}=k)}{\sum_{x,e_k(x)=y}\operatorname{prob}(\mathcal{P}=x)\cdot\operatorname{prob}(\mathcal{K}=k)}$$

According to these formulae the values can be easily computed. $\bigcirc$

(iii) Suppose $\operatorname{prob}(\mathcal{K}=1)=1/4$, $\operatorname{prob}(\mathcal{K}=2)=1/4$, $\operatorname{prob}(\mathcal{K}=3)=1/4$, $\operatorname{prob}(\mathcal{K}=4)=1/4$. *Do the same as in (ii).*

Solution. Straightforward. $\bigcirc$

(iv) Which of these key schedules is better for a one-time pad system?

Solution. The second keyscedule is better suited for a one-time pad, since the one-time pad remains perfectly secure. $\bigcirc$

Exercise 4.3 (Homework: Retail-CBC-MAC). (7 points)

7 Suppose that the CBC-MAC is combined with CBC encryption with IV $= 0$. Consider the following attack (taken from the lecture): For $k_1 = k_2 = k$ we have MAC$(p_1, p_2, \ldots, p_t, k) =$ Enc$(c_{t-1} \oplus p_t, k) = c_t$. If the adversary alters any blocks c_j for $j < t-1$ the CBC-MAC remains unchanged. The receiver will presumably not detect the loss of integrity.
Show that this attack also works against the strengthened CBC-MAC (Retail-CBC-MAC) if its first key k coincides with the encryption key.

Solution. Retail-CBC-MAC$(p_1, ..., p_t, (k_1, k_2)) = Enc(Dec(c_t, k_2), k_1)$, or equivalently, $c_t = Enc(Dec($Retail-CBC-MAC$(p_1, ..., p_t, (k_1, k_2)), k_1), k_2)$. Applying the latter equation to validate the Retail-CBC-MAC has the same consequences as the validation rule for the CBC-MAC from B.60.

Exercise 4.4 (Homework: Modes of operation). (13 points)

(i) Discuss advantages and disadvantages of each of the modes of operation presented in class: ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback), OFB (Output Feedback), CTR (Counter). 4

Solution. We give for every mode one advantage and one disadvantage:

ECB:

\+ No fault propagation
\- Data pattern is not hidden
\- Loss and permutation of blocks may not be detected

CBC:

\+ Different IVs give different ciphertext blocks even with identical plaintext blocks

CFB:

\+ Encryption and decryption are identical operations
\- Precomputation of key blocks is not feasible

OFB:

\+ A corrupt block will only affect the decryption of this particular block
\+ Precomputation of key blocks is feasible

- Unnoticed loss of a block cannot be compensated

CTR:

+ Random access property
- Unnoticed loss of a block cannot be compensated

○

(ii) Answer the following questions concerning error propagation for each of the aforementioned modes.

3 (a) How many text blocks are false if one of the transmitted blocks is corrupted?

Solution.

ECB	CBC	CFB	OFB	CTR
1	2	$\lceil n/r \rceil$	1	1

○

3 (b) How many text blocks are false if one of the transmitted blocks is dropped unnoticedly?

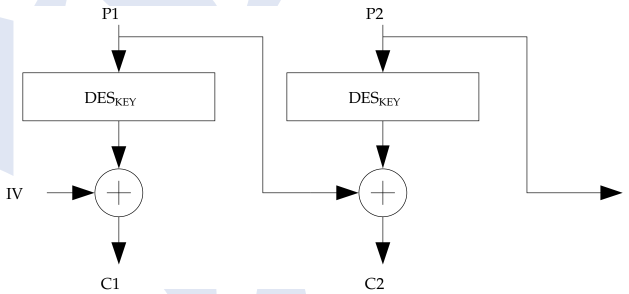
Solution.

ECB	CBC	CFB	OFB	CTR
1	2	$\lceil n/r \rceil$	∞	∞

○

Try to draw conclusions from your observations.

3 (iii) We define a further mode PBC (Plain Block Chaining) that adds the message P_i to the encrypted message C_i as depicted in the following diagram.



Answer the questions under (ii) also for this mode.

Solution. All subsequent blocks will decrypt incorrectly if there is a corrupt block or one block is lost. ○