Cryptography, winter 2006

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

2. Exercise sheet (15.11.2006)
Hand in solutions to the homework exercises on Wednesday, November 29th, in the tutorial/the lecture.

Exercise 2.1 (Repetition: Euler's φ function).

Let $p \in \mathbb{N}$ be a prime number and $m, n \in \mathbb{N}_{\geq 2}$. Euler's φ function is defined by

$$\varphi\colon \mathbb{N}_{\geq 2} \to \mathbb{N}, n \mapsto \#\left\{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\right\}.$$

Give proofs for the following formulae:

(i) $\varphi(p) = p - 1$,

Solution. In $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ every nonzero element is coprime to p, since p is prime. Thus there are $p-1$ elements $a \in \mathbb{Z}_p$ with $\gcd(a, p) = 1$. ○

(ii) $\varphi(p^e) = p^{e-1}(p-1)$ *for all* $e \in \mathbb{N}_{\geq 1}$,

Solution. If $m = p^e$ is a prime power, then the numbers that have a common factor with m are the multiples of p. There are p^{e-1} of them, so the number of factors relatively prime to p^e is $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$. ○

(iii) $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, *if* $\gcd(m, n) = 1$.

Solution. Fancy: The chinese remainder theorem says that the canonical ring homomorphism $F : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, x \mapsto (x \bmod m, x \bmod n)$ is a ring isomorphism. Write $\mathbb{Z}_n^\times := \{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$. Then $F(\mathbb{Z}_{mn}^\times) = \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$. Thus

$$\varphi(mn) = \#\mathbb{Z}_{mn}^\times = \#\mathbb{Z}_m^\times \cdot \#\mathbb{Z}_n^\times = \varphi(m) \cdot \varphi(n)$$

○

Exercise 2.2 (Combining encryption algorithms).

Assume you define the Doubled Caesar cipher *by the following encryption function, where α, β are chosen from $\mathbb{Z}_{26}$ and the function ξ is the Caesar cipher defined in exercise 1.3:*

$$\xi^{(2)}_{\alpha,\beta}\colon \mathbb{Z}_{26} \times \mathbb{Z}_{26} \to \mathbb{Z}_{26}, x \mapsto \xi_\beta(\xi_\alpha(x)).$$

(i) *Show that this cipher is as (in)secure as the Caesar cipher.*

Solution. We have $\xi_\beta(\xi_\alpha(x)) = (x+\alpha)+\beta = x+(\alpha+\beta) = \xi_{\alpha+\beta}$. $\bigcirc$

(ii) *Discuss the reasons why the combination of these two ciphers doesn't give you more security.*
Hint: *The set $\{\xi_\alpha \mid \alpha \in \mathbb{Z}_{26}\}$ forms a group with respect to composition!*

Solution. Since the set $G := \{\xi_\alpha \mid \alpha \in \mathbb{Z}_{26}\}$ forms a group with respect to composition, we have $\xi_\beta \circ G = G$, because G is closed under the operation $\circ$. Thus adding a further application of the Caesar cipher does not give anyting more than we had before. $\bigcirc$

Exercise 2.3 (Affine Codes in higher dimensions).

Consider the affine cipher over $\mathbb{Z}_{26}$ with $m = 3$. Suppose you know that the plaintext

`ADISPLAYEDEQUATION`

was encrypted to give the ciphertext

`DSRMSIOPLXLJBZULFE`

Determine the key.

Solution. We define vectors $p_1, \dots, p_4 \in \mathbb{Z}_{26}^3$ corresponding to the first four 3-blocks if the plaintext message and vectors $c_1, \dots, c_4 \in \mathbb{Z}_{26}^3$ corresponding to the first four 3-blocks if the ciphertext message as follows. The matrix $P = (p_1 - p_4 \mid p_2 - p_4 \mid p_3 - p_4)$ is given by

$$P := \begin{pmatrix} 23 & 15 & 23 \\ 25 & 11 & 20 \\ 18 & 21 & 14 \end{pmatrix}$$

The matrix $C = (c_1 - c_4 \mid c_2 - c_4 \mid c_3 - c_4)$ is given by

$$C := \begin{pmatrix} 6 & 15 & 17 \\ 25 & 7 & 4 \\ 6 & 25 & 2 \end{pmatrix}$$

By computing $A(k_1) = C \cdot P^{-1}$ we find $A(k_1)$ as

$$A(k_1) := \begin{pmatrix} 3 & 5 & 17 \\ 14 & 15 & 6 \\ 6 & 18 & 11 \end{pmatrix}$$

Substituting p_1 and c_1 in our original equation, we find $k_2 = (8, 21, 3)^T$. $\bigcirc$

Exercise 2.4 (Homework: Linear Algebra). (2 points)

$\boxed{2}$ Compute the determinant and the inverse of the following matrix A over $\mathbb{Z}_{26}$.
Hint: We are computer scientists...

$$A := \begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$$

Solution.

$$\det(A) = 5$$

$$A^{-1} := \begin{pmatrix} 25 & 11 & 22 \\ 10 & 13 & 4 \\ 17 & 24 & 1 \end{pmatrix}$$

Exercise 2.5 (Homework: Combinatorics). (8 points)

Let be $n \in \mathbb{N}$.

(i) Determine the number of permutations of a set M with n elements. Show that the set $S(M)$ of all permutations of M forms a group with respect to composition. $\boxed{4}$

Solution. Any n-set M has $n!$ permutations. The set $S(M) = \{f : M \to M \mid f \text{ bijective}\}$ of all permutations of M forms a group with respect to composition $\circ$, since the composition of two permutations is again a permutation. The permutation $f(x) = x$ that doesn't permute anything is the neutral element in this group. If you have some permuation f, the inverse map f^{-1} is the inverse element of f in $S(M)$. It exists since f is bijective. Once you have $f, g, h \in S(M)$, you find $f \circ (g \circ h) = f(g(h(x))) = (f \circ g) \circ h$. Thus $(S(M), \circ)$ is a group. Note that this group is in general not commutative.

(ii) Determine the number of possible bitstrings of length n. $\boxed{2}$

Solution. There are 2^n possible bitstrings of length n.

(iii) Determine the number of strings of length n over an alphabet Σ that do not change if they are reversed. $\boxed{2}$

Solution. Let $m = \#\Sigma$. We have two cases: If n is even, there are $m^{n/2}$ such strings. If n is odd, there are $m \cdot m^{(n-1)/2} = m^{(n+1)/2}$ such strings.

Exercise 2.6 (Homework: Substitution Cipher). (5 points)

5 The following table gives the frequency distribution of the 26 letters in typical English texts:

letter	probability	letter	probability
A	0.082	N	0.067
B	0.015	O	0.075
C	0.028	P	0.019
D	0.043	Q	0.001
E	0.127	R	0.060
F	0.022	S	0.063
G	0.020	T	0.091
H	0.061	U	0.028
I	0.070	V	0.010
J	0.002	W	0.023
K	0.008	X	0.001
L	0.040	Y	0.002
M	0.024	Z	0.001

Suppose you know that the plaintext of the following ciphertext, taken from "The Diary of Samuel Marchbanks" by. R. Davies and C. Irwin, was encrpyted using a substitution cipher (i.e. the improved variant of Caesar's cipher). You can find this text on the tutorial's webpage.

```
EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCK
QPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCG
OIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU
GFZCCMDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNS
ACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNC
IACZEJNCSHFZEJZEGMXCYHCJUMGKUCY
```

Find the plaintext!
Hint: F decrypts to W.

Solution. MAY NOT BE ABLE TO GROW FLOWERS BUT MY GARDEN PRODUCES JUST AS MANY DEAD LEAVES OLD OVERSHOES PIECES OF ROPE AND BUSHELS OF DEAD GRASS AS ANYBODYS AND TODAY I BOUGHT A WHEEM BARROW TO HELP IN CLEARING IT UP I HAVE ALWAYS LOVED AND RESPECTED THE WHEELBARROW IT IS THE ONE WHEELED VEHICLE OF WHICH I AM PERFECT MASTER

Exercise 2.7 (Homework: Combining encryption algorithms). (5 points)

Assume you encrypt a text using first the Vigenère cipher followed by an application of the Caesar cipher. Discuss whether the resulting encryption algorithm is more secure than the Caesar/the Vigenère cipher. 5

Solution. Once one has formalized the question, it is easy to see that the composition of the Caesar cipher with a Vigenère cipher is nothing but another Vigenère cipher. Thus this composition is more secure than the Caesar cipher, but only as secure as the Vigenère cipher itself.