Univ.-Prof. Dr. rer. nat. Rudolf Mathar

1	2	3	4	$\sum$
15	15	15	15	60

Written Examination

Cryptography

Tuesday, August 29, 2017, 01:30 p.m.

Name: ____________________ Matr.-No.: ____________

Field of study: ______________________________

Please pay attention to the following:

1) The exam consists of **4 problems**. Please check the completeness of your copy. **Only** written solutions on these sheets will be considered. Removing the staples is **not** allowed.

2) The exam is passed with at least **30 points**.

3) You are free in choosing the order of working on the problems. Your solution shall clearly show the approach and intermediate arguments.

4) **Admitted materials:** The sheets handed out with the exam and a non-programmable calculator.

5) The results will be published on Wednesday, the 06.09.17, 16:00h, on the homepage of the institute.

The corrected exams can be inspected on Friday, 08.09.17, 10:00h. at the seminar room 333 of the Chair for Theoretical Information Technology, Kopernikusstr. 16.

Acknowledged: ______________________________

(Signature)

Problem 1. (15 points)

a) **(8P)** Suppose that $\mathbb{P}(\hat{M} = 1) = p$ and $\hat{K}$ is uniformly distributed over the key space. $H(\hat{M}), H(\hat{K}), H(\hat{C})$. and the key equivocation $H(\hat{K} \mid \hat{C})$.

$$H(\hat{M}) = -p\log(p) - (1-p)\log(1-p)$$
$$H(\hat{K}) = \log 3$$

Note that:

$$\mathbb{P}(\hat{C} = 1) = \mathbb{P}(\hat{M} = 1, \hat{K} = k_1) = p \times \frac{1}{3} = \frac{p}{3}$$
$$\mathbb{P}(\hat{C} = 2) = \mathbb{P}(\hat{M} = 1, \hat{K} = k_2) + \mathbb{P}(\hat{M} = 2, \hat{K} = k_1) = p \times \frac{1}{3} + (1-p) \times \frac{1}{3} = \frac{1}{3}$$
$$\mathbb{P}(\hat{C} = 3) = \mathbb{P}(\hat{M} = 1, \hat{K} = k_3) + \mathbb{P}(\hat{M} = 2, \hat{K} = k_2) = p \times \frac{1}{3} + (1-p) \times \frac{1}{3} = \frac{1}{3}$$
$$\mathbb{P}(\hat{C} = 4) = \mathbb{P}(\hat{M} = 2, \hat{K} = k_3) = (1-p) \times \frac{1}{3} = \frac{1-p}{3}.$$

Hence

$$H(\hat{C}) = -\frac{p}{3}\log\frac{p}{3} - \frac{1}{3}\log\frac{1}{3} - \frac{1}{3}\log\frac{1}{3} - \frac{1-p}{3}\log\frac{1-p}{3}.$$

or

$$H(\hat{C}) = \log 3 - \frac{p}{3}\log p - \frac{1-p}{3}\log(1-p).$$

b) **(4P)** The key equivocation is given by:

$$\begin{aligned} H(\hat{K} \mid \hat{C}) &\overset{\text{Thm. 4.7}}{=} H(\hat{M}) + H(\hat{K}) - H(\hat{C}) \\ &= -p\log(p) - (1-p)\log(1-p) + \log 3 + \frac{p}{3}\log\frac{p}{3} \\ &+ \frac{1}{3}\log\frac{1}{3} + \frac{1}{3}\log\frac{1}{3} + \frac{1-p}{3}\log\frac{1-p}{3} \\ &= \frac{2}{3}(-p\log(p) - (1-p)\log(1-p)). \end{aligned}$$

$$\begin{aligned} H(\hat{M} \mid \hat{C}) &= H(\hat{C} \mid \hat{M}) + H(\hat{M}) - H(\hat{C}) \\ &= H(\hat{C} \mid \hat{M}) - \log 3 + \frac{2}{3}(-p\log(p) - (1-p)\log(1-p)). \end{aligned}$$

But $\mathbb{P}(\hat{C} = i \mid \hat{M} = j) = \frac{1}{3}$ for all i such that there is a key k for which $e(j,k) = i$. Hence:

$$H(\hat{C} \mid \hat{M}) = \log 3.$$

and

$$H(\hat{M} \mid \hat{C}) = \frac{2}{3}(-p\log(p) - (1-p)\log(1-p)).$$

c) **(3P)** The system does not have a prefect secrecy since $H(\hat{M} \mid \hat{C}) \neq H(\hat{M})$.

There is no perfect secrecy achieving key distribution in this case since we have always $|\mathcal{K}_+| < |\mathcal{C}_+|$.

Problem 2. (15 points)

a) (4P) Suppose that $a^2 \equiv r^2 (\mod n)$. Then

$$pq \mid (a-r)(a+r).$$

First if $p \mid a-r$ and $p \mid a+r$ then $p \mid 2r$. But $\gcd(p,2)=1$ and $\gcd(p,r)=1$ (since $r \in \mathbb{Z}_n^*$). Hence either $p \mid a-r$ or $p \mid a+r$ but not both. Same holds for q.

Now suppose that both $p \mid a-r$ and $q \mid a-r$. But then $pq \mid a-r$ which means that $a \equiv r (\mod n)$. But this has been excluded. Hence either $p \nmid a-r$ or $q \nmid a-r$ which means that either $p \mid a+r$ or $q \mid a+r$.

Consider an RSA cryptosystem with two prime numbers $p = 13$ and $q = 19$. The public key is given by $(n = 13 \times 19 = 247, e = 59)$.

b) (4P) The decryption exponent d is the inverse of encryption exponent modulo $\phi(n)$. First

$$\phi(pq) = (p-1)(q-1) = 12 \times 18 = 216.$$

We fine $d = e^{-1}$ using extended Euclidean Algorithm.

$$\begin{aligned} 216 &= 3 \times 59 + 39 \\ 59 &= 1 \times 39 + 20 \\ 39 &= 1 \times 20 + 19 \\ 20 &= 1 \times 19 + 1 \end{aligned}$$

Hence

$$\begin{aligned} 1 &= 20 - 1 \times 19 \\ &= 20 - 1 \times (39 - 20) = -39 + 2 \times 20 \\ &= -39 + 2 \times (59 - 39) = -3 \times 39 + 2 \times 59 \\ &= 2 \times 59 - 3 \times (216 - 3 \times 59) = 11 \times 59 - 3 \times 216 \end{aligned}$$

So $d = e^{-1} = 11$.

c) (3P) To decrypt the ciphertext $c = 10$, we need to find $c^{11} \mod 247$. To use the Square-and-Multiply Algorithm, we represent 11 in terms of powers of 2.

$$11 = 2^3 + 2 + 1 = (1011)_2$$

i	x_i	y	$y^2 \mod n$	$y^2(1 + x_i \cdot (a-1)) \mod n$
3	1	1	1	10
2	0	10	100	100
1	1	100	$100^2 \mod 247 = 120$	$120 \times 10 \mod 247 = 212$
0	1	212	$212^2 \mod 247 = 237$	$237 \times 10 \mod 247 = 147.$

Algorithm 1 Square and multiply

Require: $x = (x_t, \dots, x_0) \in \mathbb{N}, a \in \mathbb{N}$
Ensure: $a^x \mod n$

$y \leftarrow a$
for $(i = t-1, i \geq 0, i\text{--})$ **do**
    $y \leftarrow y^2 \mod n$
    if $(x_i = 1)$ **then**
        $y \leftarrow y \cdot a \mod n$
    end if
end for
return y

d) **(2P)** Suppose that the plaintext m is chosen such that $\gcd(n, m) = p$ or q. Then the ciphertext $c = m^e \mod n$ satisfies $\gcd(n, c) = p$ or q. Hence given the ciphertext c, n can be decomposed into $p' = \gcd(n, c)$ and $q' = \frac{n}{\gcd(n,c)}$. After the decomposition $\phi(n)$ can be calculated. $d = e^{-1}$ then is calculated using extended Euclidean Algorithm.

e) **(2P)** First find $\gcd(n, c)$:

$$\gcd(143, 22) = 11.$$

Using this n is decomposed by $n = 11 \times 13$ giving $\phi(n) = 120$. $d = e^{-1}$ then is calculated using extended Euclidean Algorithm.

$$120 = 17 \times 7 + 1.$$

Hence $d = -17 \mod 120 = 103$.

Problem 3. (15 points)

Message $\boldsymbol{m} = (m_1 m_2, ...m_l)$, with $m_i \in \mathbb{F}_2$.
Key $\boldsymbol{k} = (k_1 k_2, ...k_n)$, with $k_i \in \mathbb{F}_2$ and $n < l$. $\Rightarrow$ Keystream $\boldsymbol{z} = (z_1, z_2, ..., z_l)$

$$z_i = k_i, \quad 1 \leq i \leq n$$
$$z_i = \sum_{j=1}^{n} s_j z_{i-j} \mod 2, \quad n < i \leq l$$
$$c_i = z_i \oplus m_i, \quad 1 \leq i \leq l$$

a) **(2P)** Decryption: $m_i = c_i \oplus z_i$.
If $\boldsymbol{k} = \boldsymbol{0} = (00...0)$, it follows $z_i = 0, \quad 1 \leq i \leq n$, and $z_i = 0, \quad n < i \leq l$ and $c_i = m_i, \quad 1 \leq i \leq l$. In this case, the plaintext is not encrypted at all.

b) **(3P)** key length $n = 4$, key $\boldsymbol{k} = (0110)$,
addition paths $s_1 = s_4 = 1$, $s_2 = s_3 = 0 \Rightarrow \boldsymbol{s} = (1001)$,
stream length $l = 20$

z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}
0	1	1	0	0	1	0	0	0	1

z_{11}	z_{12}	z_{13}	z_{14}	z_{15}	z_{16}	z_{17}	z_{18}	z_{19}	z_{20}
1	1	1	0	1	0	1	1	0	0

The summation simplifies to $z_i = \sum_{j=1}^{n} s_j z_{ij} = z_{i-1} \oplus z_{i-4}$, $4 < i \leq 20$

encryption:

$\boldsymbol{m}$	1011	0001	0100	1101	0100
$\boldsymbol{z}$	0110	0100	0111	1010	1100
$\boldsymbol{m} \oplus \boldsymbol{z}$	1101	0101	0011	0111	1000

c) **(2P)**

- The keystream repeats itself at z_{16}. Thus the period is 15;
- Number of 0s in z: 7, number of 1s in z: 8.
- n provide registers 2^n states. Therefore, the maximal period: $p_{\text{max}} = 2^n - 1 = 15$ (Minor remark: fulfilled if z_i is a *primitive polynomial*)

d) **(8P)** The given figure provides how z_i is generated from z_{i-1}, z_{i-2}, and z_{i-3} in this case:

$$z_i = z_{i-2} + z_{i-2}$$

With the formula $z_i = \sum_{j=1}^{n} s_j z_{i-j}$, with $n < i$, we obtain $s_1 = 0$, $s_2 = 1$, $s_3 = 1$, and $n = 3$, and hence:

$$f(x) = 1 + \sum_{i=1}^{n} s_i x^i = 1 + x^2 + x^3$$

To show that $f(x)$ is primitive, we need to check that $(x^q + 1)$ with $q = 2^3 - 1 = 7$ can be divided by $f(x)$ with polynomial division without remainder:

$$\begin{array}{l}
(x^7+1):(x^3+x^2+1) = x^4+x^3+x^2+1 \\
x^7+x^6+x^4 \\ \hline
x^6+x^4+1 \\
x^6+x^5+x^3 \\ \hline
x^5+x^4+x^3+1 \\
x^5+x^4+x^2 \\ \hline
x^3+x^2+1 \\
x^3+x^2+1 \\ \hline
0
\end{array}$$

Then we need to check that there is no smaller $k < q = 7$ such that $(x^k+1):p(x)$ has no remainder for $k = 6,5,4,3,2,1$:

$$\begin{array}{l}
(x^6+1):(x^3+x^2+1) = x^3+x^2+x+\frac{x^2+x+1}{x^3+x^2+1} \\
x^6+x^5+x^3 \\ \hline
x^5+x^3+1 \\
x^5+x^4+x^2 \\ \hline
x^4+x^3+x^2+1 \\
x^4+x^3+x \\ \hline
x^2+x+1 \neq 0
\end{array}$$

$$\begin{array}{l}
(x^5+1):(x^3+x^2+1) = x^2+x+1+\frac{x}{x^3+x^2+1} \\
x^5+x^4+x^2 \\ \hline
x^4+x^2+1 \\
x^4+x^3+x \\ \hline
x^3+x^2+x+1 \\
x^3+x^2+1 \\ \hline
x \neq 0
\end{array}$$

$$\begin{array}{l}
(x^4+1):(x^3+x^2+1) = x+1+\frac{x^2+x}{x^3+x^2+1} \\
x^4+x^3+x \\ \hline
x^3+x+1 \\
x^3+x^2+1 \\ \hline
x^2+x \neq 0
\end{array}$$

$$(x^3+1):(x^3+x^2+1) \neq 0$$
$$(x^2+1):(x^3+x^2+1) \neq 0$$
$$(x+1):(x^3+x^2+1) \neq 0$$

All divisions with $k < q$ have a non-zero remainder. Hence, the polynomial $f(x)$ is shown to be primitive. (Note that the division is in $\mathbb{F}_2$, i.e., the coefficients are 0 or 1 and addition behaves equivalent to substration here.)

Problem 4. (15 points)

a) (2P) Apply the encryption function.

$$\begin{aligned} n &= p \cdot q = 199 \cdot 211 = 41989\,, \\ c &= e_K(32767) = m \cdot (m+B) \mod n \\ &= 32767 \cdot (32767 + 1357) \mod 41989 \\ &\equiv 16027 \mod 41989 \end{aligned}$$

b) (7P) Start with the encryption function and solve for m.

$$\begin{aligned} c &\equiv m^2 + B \cdot m \mod n \\ c + \left(\frac{B}{2}\right)^2 &\equiv m^2 + B \cdot m + \left(\frac{B}{2}\right)^2 \mod n \\ c + \left(\frac{B}{2}\right)^2 &\equiv \left(m + \frac{B}{2}\right)^2 \mod n \end{aligned}$$

Using the Extended Euclidean Algorithm, the multiplicative inverse of 2 modulo n is calculated as $2^{-1} \equiv 20995 \mod 41989$. With

$$\begin{aligned} \tilde{c} &:= c + \left(\frac{B}{2}\right)^2 \mod n \\ &\equiv 16027 + (1357 \cdot 20995)^2 \mod n \\ &\equiv 4013 \mod n\,, \end{aligned}$$

and

$$\begin{aligned} \tilde{m} &:= m + \frac{B}{2} \mod n \\ &\equiv m + 1357 \cdot 20995 \mod n \\ &\equiv m + 21673 \mod n\,, \end{aligned}$$

we can conclude

$$\begin{aligned} \tilde{c} &\equiv \tilde{m}^2 \mod n \\ 4013 &\equiv \tilde{m}^2 \mod n\,. \end{aligned}$$

This form is the standard Rabin Cryptosystem. In order to find the square root modulo n, we use Proposition 9.4. First, find

$$1 = \underbrace{s \cdot p}_{=:b} + \underbrace{t \cdot q}_{=:a}$$

using the Extended Euclidean Algorithm.

$$\begin{aligned}
211 &= 1 \cdot 199 + 12 \\
199 &= 16 \cdot 12 + 7 \\
12 &= 1 \cdot 7 + 5 \\
7 &= 1 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
\Rightarrow 1 &= 5 - 2 \cdot 2 \\
&= 5 - 2 \cdot (7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7 \\
&= 3 \cdot (12 - 1 \cdot 7) - 2 \cdot 7 = 3 \cdot 12 - 5 \cdot 7 \\
&= 3 \cdot 12 - 5 \cdot (199 - 16 \cdot 12) = 83 \cdot 12 - 5 \cdot 199 \\
&= 83 \cdot (211 - 1 \cdot 199) - 5 \cdot 199 = 83 \cdot 211 - 88 \cdot 199 \\
\Rightarrow b &= -88 \cdot 199 = -17512 \\
a &= 83 \cdot 211 = 17513
\end{aligned}$$

Next, we calculate the square roots modulo p and q (this is Proposion 9.3).

$$\begin{aligned}
x^2 &\equiv 4013 \equiv 33 \mod p \\
\Rightarrow x_1 &= 33^{\frac{p+1}{4}} = 33^{50} \equiv 86 \mod 199 \\
x_2 &= -x_1 \equiv 113 \mod 199\,, \\
y^2 &\equiv 4013 \equiv 4 \mod q \\
\Rightarrow y_1 &= 4^{\frac{q+1}{4}} = 4^{53} \equiv 209 \mod 211 \\
y_2 &= -y_1 = 2 \mod 211
\end{aligned}$$

Then, $f_{x_i,y_j} = ax_i + by_j$ are solutions to $f^2 = 4013 \mod n$.

$$\begin{aligned}
f_{x_1,y_1} &= a \cdot x_1 + b \cdot y_1 \mod n \\
&\equiv 17513 \cdot 86 - 17512 \cdot 209 \mod 41989 \\
&\equiv 36503 - 6965 \mod 41989 \\
&\equiv 29538 \mod 41989 \\
f_{x_1,y_2} &= 17513 \cdot 86 - 17512 \cdot 2 \mod 41989 \\
&\equiv 36503 - 35024 \mod 41989 \\
&\equiv 1479 \mod 41989 \\
f_{x_2,y_1} &= 17513 \cdot 113 - 17512 \cdot 209 \mod 41989 \\
&\equiv 5486 - 6965 \mod 41989 \\
&\equiv 40510 \equiv -f_{x_1,y_2} \mod 41989 \\
f_{x_2,y_2} &= 17513 \cdot 113 - 17512 \cdot 2 \mod 41989 \\
&\equiv 5486 - 35024 \mod 41989 \\
&\equiv 12451 \equiv -f_{x_1,y_1} \mod 41989
\end{aligned}$$

With

$$\begin{aligned}\tilde{m}^2 &\equiv \tilde{c} \mod n\\ \tilde{m} &\equiv f_{x_i,y_j} \mod n\\ m_{x_i,y_j} + 21673 &\equiv f_{x_i,y_j} \mod n\\ m_{x_i,y_j} &\equiv f_{x_i,y_j} - 21673 \mod n\end{aligned}$$

the four possible messages can now be calculated.

$$\begin{aligned}m_{x_1,y_1} &= 29538 - 21673 \equiv 7865 \mod n\\ m_{x_1,y_2} &= 1479 - 21673 \equiv 21795 \mod n\\ m_{x_2,y_1} &= 40510 - 21673 \equiv 18837 \mod n\\ m_{x_2,y_2} &= 12451 - 21673 \equiv 32767 \mod n\end{aligned}$$

Message m_{x_2,y_2} is the original one, but, knowing only the cryptogram and the private key, this message cannot be identified as the original one.

Shamir's no-key protocol with the parameters: $p = 31883, a = 8647, b = 10931, c_1 = 26843$.

c) (6P)

$$\begin{aligned}c_2 &= c_1^b \mod p = 26843^{10931} \mod 31883 \equiv 27084\\ c_3 &= c_2^{a^{-1}} \mod p = 27084^{30315} \mod 31883 \equiv 13230 \text{ (given by hint)}\\ m &= c_3^{b^{-1}} \mod p = 13230^{35} \mod 31883 \equiv 15369 \text{ (Calculator-solvable)}\\ c_1 &= m^a \mod p = 15369^{8647} \mod 31883 \equiv 26843 \text{ (To verify the solution)}\end{aligned}$$

To compute c_2 we use the square-and-multiply algorithm (SAM) (in chart):

The binary representation of $b = 10931$ is 10101010110011_2.

op	exp	modulo
1	1	26843
S	0	22732
SM	1	30451
S	0	10112
SM	1	4865
S	0	11039
SM	1	31241
S	0	29568
SM	1	18408
SM	1	10481
S	0	14426
S	0	9135
SM	1	24741
SM	1	27084

To compute a^{-1} modulo $p - 1$, we first derive equations from Extended Euclidean

Algorithm (EEA) as follows:

$$\begin{aligned}
31882 &= 3 \times 8647 + 5941 \\
8647 &= 5941 + 2705 \\
5941 &= 2 \times 2706 + 529 \\
2706 &= 5 \times 529 + 61 \\
529 &= 8 \times 61 + 41 \\
61 &= 41 + 20 \\
41 &= 2 \times 20 + 1 \Rightarrow \gcd(31882, 8647) = 1,
\end{aligned}$$

then we substitute the factors backwards:

$$\begin{aligned}
1 &= 41 - 2 \times 20 \\
&= 41 - 2 \times (61 - 41) = 3 \times 41 - 2 \times 61 \\
&= 3 \times (529 - 8 \times 61) - 2 \times 61 = 3 \times 529 - 26 \times 61 \\
&= 133 \times 529 - 26 \times 2706 \\
&= 133 \times 5941 - 292 \times 2706 \\
&= 425 \times 5941 - 292 \times 8647 \\
&= 425 \cdot 31882 \underbrace{-1567}_{a^{-1}} \times \underbrace{8647}_{a}
\end{aligned}$$

Hence $a^{-1} = -1567 \equiv 30315 \mod (p-1)$. Similarly, $b^{-1} = 35$

Hint: Check if result is equal to one in each step!

The exchanged value $c_3 = c_2^{a^{-1}} \mod p = 27084^{30315} \mod 31883 \equiv 13230$ is given in the question. Thus, the message is $m = c_3^{b^{-1}} \mod p = 13230^{35} \mod 31883 \equiv 15369$ which can be computed by the calculator or by the SAM algorithm.

Additional sheet

Problem:

Additional sheet

Problem:

Additional sheet

Problem: