Chair for Theoretical Information Technology | RWTH AACHEN UNIVERSITY

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

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

Written examination

Cryptography

Tuesday, August 23, 2016, 08:30 a.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 Tuesday, the 30.08.16, 16:00h, on the homepage of the institute.

The corrected exams can be inspected on Tuesday, 02.09.16, 10:00h. at the seminar room 333 of the Chair for Theoretical Information Technology, Kopernikusstr. 16.

Acknowledged: ______________________________

(Signature)

Problem 1. (15 points)

a) Using Euler's criterion, -1 is a quadratic residue iff $(-1)^{\frac{p-1}{2}} = 1$, which means $\frac{p-1}{2} = 2k$ or $p = 4k+1$. **(3P)**

b) From Wilson's theorem, it is known that: **(3P Bonus)**

$$(p-1)! \equiv -1 \mod p.$$

On the other hand see that:

$$\begin{aligned} \frac{p-1}{2} &\equiv -\frac{p+1}{2} \mod p \\ \frac{p-3}{2} &\equiv -\frac{p+3}{2} \mod p \\ &\cdots\cdots \\ 1 &\equiv -(p-1) \mod p. \end{aligned}$$

Therefore:

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2} \right)! \right)^2 \mod p.$$

If $4|p-1$, then the previous equia implies that :

$$-1 \equiv \left(\left(\frac{p-1}{2} \right)! \right)^2 \mod p.$$

c) Use chinese remainder theorem for two solutions $\left(\frac{p-1}{2}\right)!$ and $\left(\frac{q-1}{2}\right)!$. **(5P)**

d) One way is to find a from $a^2 \equiv -1 \mod n$ and then finding c/a. **(3P)** An easier way for decryption is simply by $-c^2 \mod n$. It requires that n be known at the decoder. **(1P) Bonus**

e) Since $n|a^2+1$, one can look at prime decomposition of a^2+1 to find possible $n = pq$. The attack is difficult since the decomposition is difficult. Moreover there might be multiple possibilities for n. **(4P)**

Problem 2. (15 points)

a) **(3P)**

$$H(\hat{C}|\hat{M}=M) = -\sum_{C\in\mathcal{C}} P(\hat{C}=C|\hat{M}=M)\log P(\hat{C}=C|\hat{M}=M)$$
$$= -(1-\epsilon)\log(1-\epsilon) - \epsilon\log(\frac{\epsilon}{|\mathcal{K}|-1}).$$

This is independent of $P(\hat{M}=M)$, therefore:

$$H(\hat{C}|\hat{M}) = \sum_{M\in\mathcal{M}} P(\hat{M}=M)H(\hat{C}|\hat{M}=M) = -(1-\epsilon)\log(1-\epsilon) - \epsilon\log(\frac{\epsilon}{|\mathcal{K}|-1}).$$

b) Using conditioning on $\hat{M}$: **(4P)**

$$P(\hat{C}=C) = \sum P(\hat{M}=M)P(\hat{C}=C|\hat{M}=M) = (1-\epsilon)P(\hat{M}=C) + \frac{\epsilon}{|\mathcal{K}|-1}P(\hat{M}\neq C).$$

Now see that $H(\hat{M}) - H(\hat{M}|\hat{C}) = H(\hat{C}) - H(\hat{C}|\hat{M})$.

If $\hat{M}$ is uniformly distributed, then:

$$P(\hat{C}=C) = (1-\epsilon)\frac{1}{|\mathcal{M}|} + \frac{\epsilon}{|\mathcal{K}|-1}\frac{|\mathcal{M}|-1}{|\mathcal{M}|}.$$

Since $|\mathcal{M}| = |\mathcal{K}|$, $\hat{C}$ is uniformly distributed and :

$$H(\hat{C}) = \log|\mathcal{K}|.$$

Therefore:

$$H(\hat{M}) - H(\hat{M}|\hat{C}) = \log|\mathcal{K}| + (1-\epsilon)\log(1-\epsilon) + \epsilon\log(\frac{\epsilon}{|\mathcal{K}|-1})$$
$$= \log|\mathcal{K}| - \epsilon\log(|\mathcal{K}|-1) + (1-\epsilon)\log(1-\epsilon) + \epsilon\log(\epsilon)$$
$$= \log|\mathcal{K}| - \epsilon\log(|\mathcal{K}|-1) - h_b(\epsilon),$$

where $h_b(\epsilon) = -(1-\epsilon)\log(1-\epsilon) - \epsilon\log(\epsilon)$ is the entropy of a Bernoulli RV with parameter ϵ.

c) $\log|\mathcal{K}| - \epsilon\log(|\mathcal{K}|-1) = (1-\epsilon)\log|\mathcal{K}| + \epsilon\log(\frac{|\mathcal{K}|}{|\mathcal{K}|-1})$. When $|\mathcal{K}|$ is large $\log(\frac{|\mathcal{K}|}{|\mathcal{K}|-1})$ is small and the dominant term is $(1-\epsilon)\log|\mathcal{K}|$. **(3P)**

d) When $\epsilon = 0$, then $H(\hat{M}) - H(\hat{M}|\hat{C}) = H(\hat{M})$, because we have an identity mapping. When $\epsilon = 1$, we have: **(3P)**

$$H(\hat{M}) - H(\hat{M}|\hat{C}) = \log(\frac{|\mathcal{K}|}{|\mathcal{K}|-1}).$$

As $|\mathcal{K}|$ grows large, $\log(\frac{|\mathcal{K}|}{|\mathcal{K}|-1})$ tends to zero and the system approaches the perfect secrecy.

e) The perfect secrecy is achieved when $P(\hat{C}=C|\hat{M}=M)$ does not depend on M and C. Hence: **(2P)**

$$1-\epsilon = \frac{\epsilon}{|\mathcal{K}|-1} \implies \epsilon = \frac{|\mathcal{K}|-1}{|\mathcal{K}|}.$$

Problem 3. (15 points)

a) The steps for the AES128 encryption are: **(3P)**

- Having a key size of 128 bits $\longrightarrow$ we have $r = 10$ rounds
- The steps for the rounds $1, \ldots, r-1$ consist on the following:
  - SubBytes (SB)
  - ShiftRows (SR)
  - MixColums (MC)
  - AddRoundKey (ARC)
- The last round consists of SubBytes, ShiftRows and AddRoundKey

b) The solution is: **(5P)**
$tmp \leftarrow W_3 = (69\ 74\ 6F\ 2A)_{16}$
$RotByte(tmp) = (74\ 6F\ 2A\ 69)_{16}$
$SubBytes(RotByte(tmp)) = (92\ A8\ E5\ F9)_{16}$
$Rcon(1) = (01\ 00\ 00\ 00)$
$tmp \leftarrow SubBytes(RotByte(tmp)) \oplus Rcon(\frac{i}{4}) = (93\ A8\ E5\ F9)_{16}$
$W_4 \leftarrow W_3 \oplus tmp = (69\ 20\ E2\ 99) \oplus tmp = (FA\ 88\ 07\ 60)_{16}$

c) The keys $K_, \ldots, K_{16}$ are all the same (all 1ss). Decryption is accomplished by reversing the order of the keys to $K_{16}, \ldots, K_1$. Since the K_i are all the same, this is the same as encryption, so encrypting twice gives back the plaintext. **(2P)**

d) The key of all 0s, by the same reasoning as before. **(2P)**

e) No, this problem does not persist due to the key expansion algorithm, since the key expansion makes the rounds no longer corresponding one-to-one with other lengths bit-keys. **(3P)**

Problem 4. (15 points)

a) We have $\alpha = (5n + 7)$ and $\beta = (3n + 4)$ **(3P)**

The Bezout lemma states that iff a and b are coprime then the following equation has integer solutions:

$$\alpha \cdot x + \beta \cdot y = 1$$

Therefore,

$$(5n + 7) \cdot x + (3n + 4) \cdot y = 1$$

Now, we apply the EEA to the previous equation:

$$\begin{aligned}
(5n + 7) &= (3n + 4) + (2n + 3) \\
(3n + 4) &= (2n + 3) + (n + 1) \\
(2n + 3) &= 2(n + 1) + 1
\end{aligned}$$

Now backwards:

$$\begin{aligned}
1 &= (2n + 3) - 2(n + 1) \\
&= (2n + 3) - 2(-(2n + 3) + (3n + 4)) \\
&= 3(2n + 3) - 2(3n + 4) \\
&= (2n + 3) + 2(2n + 3) - 2(3n + 4) \\
&= 3(2n + 3) - 2(3n + 4) \\
&= 3((5n + 7) - (3n + 4)) - 2(3n + 4) \\
&= 3(5n + 7) - 3(3n + 4) - 2(3n + 4) \\
&= 3(5n + 7) - 5(3n + 4)
\end{aligned}$$

Therefore, $x = 3$ and $y = -5$ which prove that α and β are relatively prime

b) The steps to generate the first prime p are the following: **(3P)**

- Using a random number generator, we generate a random number of size $K/2$
- Set the lowest bit of the generated integer to ensure that the number will be odd
- Set the two highest bits of the integer to ensure that the highest bits of n will be set
- Using the MRPT, we check if the resulting integer is prime. If not, we increment the value by 2 and check again

The entire procedure is analogous for q.

c) The given RSA cryptosystem has the following parameters: **(3P)**

$p = 11$, $q = 13$, $e = 7$ and $n = p \cdot q = 143$

Using the Euler function: $\phi(n) = 10 \cdot 12 = 120$

Having the expression: $m = c^d \bmod n$, we need to calculate the $gdc(e, \phi(n)) = 1$

$$\begin{aligned} 120 &= 17 \cdot 7 + 1 \\ 7 &= 1 \cdot 6 + 1 \end{aligned}$$

Now backwards

$$\begin{aligned} 1 &= 7 - (1 \cdot 6) \\ &= 7 - 6(120 - 17 \cdot 7) \\ &= 7 - (6 \cdot 120) + 102 \cdot 7 \\ &= 103 \cdot 7 - 6 \cdot 120 \longrightarrow d = 103 \end{aligned}$$

$m \equiv c^d \bmod n \equiv 31^{103} \bmod 143$. Therefore, applying the SM algorithm we obtain $m = 47$

d) Since $gcd(e_A, e_B) = 1$, there exist integers x and y with $e_A \cdot x + e_B \cdot y$. Therefore, $m = m^1 = m^{e_A \cdot x + e_B \cdot y} = (m^{e_A})^x \cdot (m^{e_B})^y \equiv {c_A}^x \cdot {c_B}^y$. Since Claire has access to the values c_A and c_B she can calculate m. **(2P)**

e) The requirements of a digital signature are: **(2P)**

- it must be verifiable
- it must be forgery-proof
- it must be firmly connected to the document

f) Oskar wants to obtain a chosen signature $s = m^d \bmod n$ **(2P)**

- Oskar generates a message $m_2 = m \cdot m^{-1} \bmod n$ and asks again to sign a message m_2, obtaining $s_2 = {m_2}^d \bmod n$
- From the pairs (m_1, s_1) and (m_2, s_2) the wanted signature s on message m can be recovered as $s = s_1 \cdot s_2 \bmod n$

Proof :

$$\begin{aligned} s &\equiv s_1 \cdot s_2 \equiv {m_1}^d \cdot {m_2}^d \equiv {m_1}^d \cdot (m \cdot m^{-1})^d \equiv \\ &\equiv {m_1}^d \cdot m^d \equiv m^d \mathrm{mod} n \end{aligned}$$