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

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) Prove that -1 is a quadratic residue mod p if and only if $p = 4k + 1$ for some $k \in \mathbb{N}$.

b) Show that if $p = 4k + 1$, then $x = \left(\frac{p-1}{2}\right)!$ is a solution to $x^2 \equiv -1 \mod p$.
(Hint: Use Wilson's theorem; see below)

c) For $n = pq$ with $p = 4k+1$ and $q = 4k'+1$ for some integers k and k', find a solution for $x^2 \equiv -1 \mod n$.

Consider a cryptosystem with the following protocol:

- Choose prime numbers p and q such that for some $k, k' \in \mathbb{N}$, $p = 4k + 1$ and $q = 4k' + 1$. Let $n = pq$.
- Choose the number a such that it is a solution to $a^2 \equiv -1 \mod n$.
- The private key is n, known for decryption.
- A message m is assumed to be one of the quadratic residues modulo n. Choose $x \in \mathbb{Z}_n^*$ such that $x^2 \equiv m \mod n$.
- The encryption function is defined by $c = ax$ (not taken modulo n).

d) Propose a decryption function for this cryptosystem.

e) If a is public, then propose an attack against this cryptosystem. Discuss the complexity of this attack.

Wilson's theorem: $(p-1)! \equiv -1 \mod p$, if p is prime.

Problem 2. (15 points)
Let $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ be a cryptosystem such that $P(\hat{M} = M) > 0$ for all $M \in \mathcal{M}$ and $P(\hat{K} = K) > 0$ for all $K \in \mathcal{K}$. Also suppose that $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. Suppose that the message and the ciphertext are related as follows for some $\epsilon \in [0, 1]$:

$$P(\hat{C} = M|\hat{M} = M) = 1 - \epsilon$$

and if $M' \neq M$:

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

a) Show that $H(\hat{C}|\hat{M})$ does not depend on the probability distribution over the message space $P(\hat{M} = M)$.

b) Find $P(\hat{C} = C)$ for an arbitrary distribution over the message space. If the messages are uniformly distributed over the message space, i.e., $P(\hat{M} = M) = \frac{1}{|\mathcal{M}|}$, show that:

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

For the following suppose that the messages are uniformly distributed over the message space.

c) Show that $H(\hat{M}) - H(\hat{M}|\hat{C})$ increases linearly with $\log|\mathcal{K}|$ for large $|\mathcal{K}|$. In other words, show that:

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

d) Discuss the secrecy for ϵ equal to 0 and 1. Show that for $\epsilon = 1$, as $|\mathcal{K}|$ grows, the cryptosystem approaches perfect secrecy, i.e., $\lim_{|\mathcal{K}| \to \infty}\left[H(\hat{M}) - H(\hat{M}|\hat{C})\right] = 0$.

e) For which ϵ is perfect secrecy achieved in this system?

Problem 3. (15 points)

Consider the Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

a) What are the steps in each round of the encryption procedure of AES128?.

b) In the case of AES128, a key expansion operation is performed from the following master key:

$$K = 69\ 20\ E2\ 99\ A5\ 20\ 2A\ 6D\ 65\ 6E\ 63\ 68\ 69\ 74\ 6F\ 2A$$

What are the first 4 bytes of K_1?
Hint: Use the algorithm described below.

c) Let K be a DES key consisting of all 1s, and E_K be the encryption function of DES. Show that if the plaintext P is encrypted twice, the final ciphertext is the plaintext P, i.e., if $E_K(P) = C$, then $E_K(C) = P$.

d) Find another example of a key with the same property, namely find K such that $E_K(P) = C$ then $E_K(C) = P$.

e) Suppose that the above key K is used in AES with the corresponding encryption function E_K. If $C = E_K(P)$, does it hold in general that $E_K(C) = P$? Substantiate your answer.

Hint: Use the following algorithm for the key expansion operation

---

Split K into 4 32-bit words W_0, W_1, W_2, W_3
for $(i \leftarrow 4;\ i < 4 \cdot (r+1);\ i++)$ **do**
  tmp $\leftarrow W_{i-1}$
  if $(i \mod 4 = 0)$ **then**
    tmp $\leftarrow$ `SubBytes`(`RotByte`(tmp)) $\oplus$ `Rcon`$(i/4)$
  end if
  $W_i \leftarrow W_{i-4} \oplus$ tmp
end for

For this task, you can use the table for the SubBytes operation and also the following functions Rcon and RotByte:

- RotByte is a cyclic leftshift by one byte.
- $\text{Rcon}(i) = (\text{RC}(i), 0\text{x}00, 0\text{x}00, 0\text{x}00)$.
- $\text{RC}(i)$ representing x^{i-1} as element of $\mathbb{F}_{2^8}$.

`SubBytes`

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Problem 4. (15 points)

a) Show that $\alpha = 5n + 7$ and $\beta = 3n + 4$ are relatively prime for any integer n.
Hint: If $\alpha \cdot x + \beta \cdot y = 1$ for some integers x and y then α and β are relatively prime.

b) Alice and Bob use the RSA cryptosystem and hence need to choose two prime numbers p and q. Using the Miller-Rabin Primality Test, describe a method to generate the prime numbers p and q, such that $n = pq$ has exactly K bits and p and q have $K/2$ bits, provided K is even.

c) Alice and Bob choose prime numbers $p = 11$ and $q = 13$. Moreover, Alice chooses her private key as $e = 7$. Bob receives a ciphertext $c = 31$. What is the message m sent by Alice?.

d) Suppose Alice and Bob use the RSA system with the same modulo n and their public keys e_A and e_B are relatively prime. A new user Claire wants to send a message to both Alice and Bob, so Claire encrypts the message using $c_A = m^{e_A}$ mod n and $c_B = m^{e_B}$ mod n. Show how an eavesdropper can decipher the message m by intercepting both c_A and c_B.

Consider the RSA signature scheme.

e) Describe the requirements of a *digital signature*.

f) Suppose that Oscar is interested in knowing Alice's signature s for the message m. Oscar knows Alice's signatures for the messages m_1 and $m_2 = (m \cdot {m_1}^{-1})$ mod n, where ${m_1}^{-1}$ is the inverse of m_1 modulo n. Show that Oscar can generate a valid signature s on m, using the signatures of m_1 and m_2.