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 $x^2 \equiv -1 \pmod{p}$.
   (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 $x^2 \equiv -1 \pmod{n}$.

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 $a^2 \equiv -1 \pmod{n}$.
- 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 $x^2 \equiv m \pmod{n}$.
- 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: $(p - 1)! \equiv -1 \pmod{p}$, 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 \(\epsilon\) equal to 0 and 1. Show that for \(\epsilon = 1\), as \(|\mathcal{K}|\) grows, the cryptosystem approaches perfect secrecy, i.e., \(\lim_{|\mathcal{K}| \to \infty} [H(\hat{M}) - H(\hat{M} | \hat{C})] = 0\).

e) For which \(\epsilon\) 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 $(i ← 4; i < 4 \cdot (r + 1); i + +)$ do

  tmp ← $W_{i-1}$

  if $(i \mod 4 = 0)$ then

    tmp ← SubBytes(RotByte(tmp)) ⊕ Rcon(i/4)

  end if

  $W_i$ ← $W_{i-4} ⊕$ 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.
- $Rcon(i) = (RC(i), 0x00, 0x00, 0x00)$.
- $RC(i)$ representing $x^{i-1}$ as element of $\mathbb{F}_{2^8}$. 
<table>
<thead>
<tr>
<th></th>
<th>99</th>
<th>124</th>
<th>119</th>
<th>123</th>
<th>242</th>
<th>107</th>
<th>111</th>
<th>197</th>
<th>48</th>
<th>1</th>
<th>103</th>
<th>43</th>
<th>254</th>
<th>215</th>
<th>171</th>
<th>118</th>
</tr>
</thead>
<tbody>
<tr>
<td>202</td>
<td>130</td>
<td>201</td>
<td>125</td>
<td>250</td>
<td>89</td>
<td>71</td>
<td>240</td>
<td>173</td>
<td>212</td>
<td>162</td>
<td>175</td>
<td>156</td>
<td>164</td>
<td>114</td>
<td>192</td>
<td></td>
</tr>
<tr>
<td>183</td>
<td>253</td>
<td>147</td>
<td>38</td>
<td>54</td>
<td>63</td>
<td>247</td>
<td>204</td>
<td>52</td>
<td>165</td>
<td>229</td>
<td>241</td>
<td>113</td>
<td>216</td>
<td>49</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>209</td>
<td>0</td>
<td>237</td>
<td>32</td>
<td>252</td>
<td>177</td>
<td>91</td>
<td>106</td>
<td>203</td>
<td>190</td>
<td>57</td>
<td>74</td>
<td>76</td>
<td>88</td>
<td>207</td>
<td></td>
</tr>
<tr>
<td>208</td>
<td>239</td>
<td>170</td>
<td>251</td>
<td>67</td>
<td>77</td>
<td>51</td>
<td>133</td>
<td>69</td>
<td>249</td>
<td>2</td>
<td>127</td>
<td>80</td>
<td>60</td>
<td>159</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>163</td>
<td>64</td>
<td>143</td>
<td>146</td>
<td>157</td>
<td>56</td>
<td>245</td>
<td>188</td>
<td>182</td>
<td>218</td>
<td>33</td>
<td>16</td>
<td>255</td>
<td>243</td>
<td>210</td>
<td></td>
</tr>
<tr>
<td>205</td>
<td>12</td>
<td>19</td>
<td>236</td>
<td>95</td>
<td>151</td>
<td>68</td>
<td>23</td>
<td>196</td>
<td>167</td>
<td>126</td>
<td>61</td>
<td>100</td>
<td>93</td>
<td>25</td>
<td>115</td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>129</td>
<td>79</td>
<td>220</td>
<td>34</td>
<td>42</td>
<td>144</td>
<td>136</td>
<td>70</td>
<td>238</td>
<td>184</td>
<td>20</td>
<td>222</td>
<td>94</td>
<td>11</td>
<td>219</td>
<td></td>
</tr>
<tr>
<td>224</td>
<td>50</td>
<td>58</td>
<td>10</td>
<td>73</td>
<td>6</td>
<td>36</td>
<td>92</td>
<td>194</td>
<td>211</td>
<td>172</td>
<td>98</td>
<td>145</td>
<td>149</td>
<td>228</td>
<td>121</td>
<td></td>
</tr>
<tr>
<td>231</td>
<td>200</td>
<td>55</td>
<td>109</td>
<td>141</td>
<td>213</td>
<td>78</td>
<td>169</td>
<td>108</td>
<td>86</td>
<td>244</td>
<td>234</td>
<td>101</td>
<td>122</td>
<td>174</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>186</td>
<td>120</td>
<td>37</td>
<td>46</td>
<td>28</td>
<td>166</td>
<td>180</td>
<td>198</td>
<td>232</td>
<td>221</td>
<td>116</td>
<td>31</td>
<td>75</td>
<td>189</td>
<td>139</td>
<td>138</td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>62</td>
<td>181</td>
<td>102</td>
<td>72</td>
<td>3</td>
<td>246</td>
<td>14</td>
<td>97</td>
<td>53</td>
<td>87</td>
<td>185</td>
<td>134</td>
<td>193</td>
<td>29</td>
<td>158</td>
<td></td>
</tr>
<tr>
<td>225</td>
<td>248</td>
<td>152</td>
<td>17</td>
<td>105</td>
<td>217</td>
<td>142</td>
<td>148</td>
<td>155</td>
<td>30</td>
<td>135</td>
<td>233</td>
<td>206</td>
<td>85</td>
<td>40</td>
<td>223</td>
<td></td>
</tr>
<tr>
<td>140</td>
<td>161</td>
<td>137</td>
<td>13</td>
<td>191</td>
<td>230</td>
<td>66</td>
<td>104</td>
<td>65</td>
<td>153</td>
<td>45</td>
<td>15</td>
<td>176</td>
<td>84</td>
<td>187</td>
<td>22</td>
<td></td>
</tr>
</tbody>
</table>
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 \( \alpha \) and \( \beta \) 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 \( m_2 \).