Instructor: Fatih Temiz
Due Date: May 5, 18:00

Full Name:
Student No:
Department:

INSTRUCTIONS: You must write GOOD mathematics; clear, meaningful, consistent. Show each step of your work to receive full credit. If you use a programming platform for a computation, write the set of commands that produced the result. Upload a SINGLE PDF file. It must be readable. No late homework is accepted.

Question:	1	2	3	4	Total
Points:	25	35	25	35	120
Result:					

1. (25 points) There are ciphertexts in the attached pdf file. Look at your row number (between 1 and 166) in the Tables 1, 2 or 3 and find your own ciphertext in the attached file. Decrypt your own ciphertext obtained from a Substitution Cipher.
   Note that there may be meaningless words at the beginning or at the end since the plaintext is divided into equal parts.

2. (35 points) Find the S-Box output of the input which you will obtain by following the steps:
   (a) Take the last 8 digits of your student number and take mod 2 of each digit.
   (b) Convert your row number (1 to 166) to binary string of length 8 (by padding the first digits with 0's if needed).
   (c) XOR these two binary strings.
   (d) Find this binary string's correspondent polynomial in the filed $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/ < x^8 + x^4 + x^3 + x + 1 >$.
   (e) Find the inverse of this polynomial in $\mathbb{F}_{2^8}$ and convert it to binary.

3. (25 points) Find your own prime number p in the Table.
   (a) Consider the multiplicative group $\mathbb{F}_p^*$ and find a generator (primitive root) of it.
   Hint: $\mathbb{F}_p^*$ has $\phi(p) = p - 1$ elements and the order of an element must divide the order of group.
   (b) Use the extended Euclidean Algorithm to compute the inverse of 5 mod p.

4. (35 points) Find your own prime number q in the Table.
   (a) Consider the multiplicative group $\mathbb{F}_q^*$ and find a generator (primitive root) of it.
   (b) Show the steps of the Diffie-Hellman between Alice and Bob such that they choose the secret values as $a = 32$ and $b = 64$. What are the values of $A = g^a$ and $B = g^b$. What is the agreed key?
   (c) Use Fermat's Little Theorem to compute the inverse of 7 mod q.

	Student No	Full Name	p	q
1	160201047	BE**** ÖZ****	73	1109
2	170201012	MU**** AL****	79	1103
3	170201032	ED**** GÖ****	83	1097
4	170201057	MU**** DO****	89	1093
5	170209002	AH**** BU****	97	1091
6	170209003	BA**** BO****	101	1087
7	170209004	HÜ**** AL****	103	1069
8	170209005	CU**** GÜ****	107	1063
9	170209006	ÇA**** ŞE****	109	1061
10	170209007	FA**** ÖZ****	113	1051
11	170209008	HA**** GÜ****	127	1049
12	170209009	BU**** AN****	131	1039
13	170209010	SE**** YI****	137	1033
14	170209011	KA**** GÜ****	139	1031
15	170209013	FU**** KA****	149	1021
16	170209014	MA**** GÖ****	151	1019
17	170209015	FA**** GÜ****	157	1013
18	170209016	ÖM**** HA****	163	1009
19	170209017	AZ**** AD****	167	997
20	170209018	MU**** Şİ****	173	991
21	170209019	ON**** TO****	179	983
22	170209021	İS**** KA****	181	977
23	170209022	MÜ**** ÖZ****	191	971
24	170209024	YA**** PO****	193	967
25	170209025	SA**** AY****	197	953
26	170209026	DA**** ÖĞ****	199	947
27	170209028	BU**** YI****	211	941
28	170209029	SÜ**** ŞE****	223	937
29	170209030	RI**** TE****	227	929
30	170209031	SE**** UG****	229	919
31	170209032	EM**** KA****	233	911
32	170209034	BE**** KI****	239	907
33	170209035	ME**** EK****	241	887
34	170209037	ZE**** YÜ****	251	883
35	170209039	BU**** KA****	257	881
36	170209922	JO**** ZO****	263	877
37	170209924	AS**** AS****	269	863
38	170209930	MU**** AL****	271	859
39	170209934	IL**** FA****	277	857
40	180201004	EL**** UZ****	281	853
41	180201006	ME**** ŞE****	283	839
42	180201010	AS**** GÜ****	293	829
43	180201011	AY**** DO****	307	827
44	180201013	ÖZ**** ÇI****	311	823
45	180201015	İR**** GÜ****	313	821
46	180201017	OĞ**** AK****	317	811
47	180201020	EN**** TI****	331	809
48	180201025	ZE**** KO****	337	797
49	180201028	YA**** KA****	347	787
50	180201029	ME**** YA****	349	773
51	180201034	FA**** YO****	353	769
52	180201035	MU**** UZ****	359	761
53	180201037	AL**** KA****	367	757
54	180201039	ME**** OR****	373	751
55	180201043	AH**** AK****	379	743
56	180201045	Dİ**** BO****	383	739
57	180201046	İH**** KU****	389	733
58	180201049	BE**** AK****	397	727
59	180201050	NU**** DE****	401	719
60	180201054	AS**** HO****	409	709

Table 1: Prime Numbers p and q which will be used in problems

	Student No	Full Name	p	q
61	180201055	ME**** BU****	419	701
62	180201057	SE**** KO****	421	691
63	180201058	Sİ**** VA****	431	683
64	180201063	YU**** ÜN****	433	677
65	180201069	UM**** DE****	439	673
66	180201071	EM**** DA****	443	661
67	180201072	ON**** ÇA****	449	659
68	180201807	Bİ**** ÖZ****	457	653
69	180201908	TA**** AL****	461	647
70	180201911	ZA**** KA****	463	643
71	180201920	AH**** SH****	467	641
72	180201945	OM**** SA****	479	631
73	180209003	Cİ**** DE****	487	619
74	180209012	AT**** IŞ****	491	617
75	180209015	Nİ**** AR****	499	613
76	180209021	Nİ**** AK****	503	607
77	180209031	SE**** YI****	509	601
78	180209034	MU**** BA****	521	599
79	180209035	HA**** AÇ****	523	593
80	180209037	İR**** BU****	541	587
81	180209049	HA**** DE****	547	577
82	180209801	YU**** TO****	557	571
83	180209804	CA**** TA****	563	569
84	180209904	FA**** AB****	569	563
85	180209905	YA**** AL****	571	557
86	180209907	MO**** JA****	577	547
87	180209916	TA**** AL****	587	541
88	180209917	AB**** AB****	593	523
89	180209925	AD**** DA****	599	521
90	180209928	YO**** MO****	601	509
91	180209929	AB**** AL****	607	503
92	180209932	AH**** AH****	613	499
93	180209933	MO**** EL****	617	491
94	180209934	OM**** GH****	619	487
95	180209935	MO**** AL****	631	479
96	180209939	RE**** MO****	641	467
97	180209945	RA**** OB****	643	463
98	180209947	IB**** IB****	647	461
99	180209952	SA**** SA****	653	457
100	180209953	AH**** SA****	659	449
101	180209956	SA**** SA****	661	443
102	190104056	PE**** TA****	673	439
103	190200013	BE**** SA****	677	433
104	190200014	ZE**** BA****	683	431
105	190200015	EZ**** ÖZ****	691	421
106	190200016	İR**** ÇE****	701	419
107	190200035	AS**** GÜ****	709	409
108	190201007	EY**** ZE****	719	401
109	190201010	SE**** TÜ****	727	397
110	190201011	HA**** KA****	733	389
111	190201015	ME**** AT****	739	383
112	190201026	KE**** ŞA****	743	379
113	190201029	MU**** ÇE****	751	373
114	190201030	AY**** TE****	757	367
115	190201035	AH**** GÜ****	761	359
116	190201038	MU**** DU****	769	353
117	190201051	MU**** ÇO****	773	349
118	190201055	EM**** TA****	787	347
119	190201056	ŞE**** İN****	797	337
120	190201057	ÇA**** ÇE****	809	331

Table 2: Prime Numbers p and q which will be used in problems

	Student No	Full Name	p	q
121	190201060	SE**** KI****	811	317
122	190201065	ÖM**** AK****	821	313
123	190201084	AY**** AK****	823	311
124	190201087	FA**** KE****	827	307
125	190201096	OM**** DA****	829	293
126	190201100	MO**** BA****	839	283
127	190201101	DA**** AK****	853	281
128	190201801	FU**** MA****	857	277
129	190201805	CE**** İN****	859	271
130	190201806	YA**** AL****	863	269
131	190201808	CA**** SE****	877	263
132	190201813	HA**** YI****	881	257
133	190201814	AR**** TE****	883	251
134	190201918	AN**** CH****	887	241
135	190201925	MO**** AL****	907	239
136	190201929	AB**** AB****	911	233
137	190201960	MO**** AB****	919	229
138	190201962	HA**** RI****	929	227
139	190201964	MO**** BE****	937	223
140	190201967	CL**** NW****	941	211
141	190201974	SE**** LI****	947	199
142	190201990	RA**** EL****	953	197
143	190201996	AY**** OS****	967	193
144	190209020	KA**** AK****	971	191
145	190209074	OU**** AL****	977	181
146	190209806	AH**** TA****	983	179
147	190209906	AH**** HA****	991	173
148	190209948	KA**** AL****	997	167
149	190209965	AB**** MI****	1009	163
150	190209975	MO**** AL****	1013	157
151	190209984	SA**** OT****	1019	151
152	200200004	SE**** ER****	1021	149
153	200201030	EL**** TU****	1031	139
154	200201341	SA**** KU****	1033	137
155	200201803	MU**** ZA****	1039	131
156	200201806	ER**** GÜ****	1049	127
157	200201939	AL**** AL****	1051	113
158	200209323	AB**** MO****	1061	109
159	200209377	EL**** AL****	1063	107
160	200209378	ME**** BU****	1069	103
161	200209381	CE**** AR****	1087	101
162	200209701	EM**** AY****	1091	97
163	210201308	AB**** AL****	1093	89
164	210201607	Sh**** Am****	1097	83
165	210201810	MU**** GÜ****	1103	79
166	210201811	Dİ**** ŞA****	1109	73

Table 3: Prime Numbers p and q which will be used in problems