Kryptologie LAB - 3.2

Summer Semester 2020

Dr. Joshua Blinkhorn

Friedrich-Schiller-Universität Jena

Data Encryption Standard (DES)

1. Key generation - 16 keys from one key

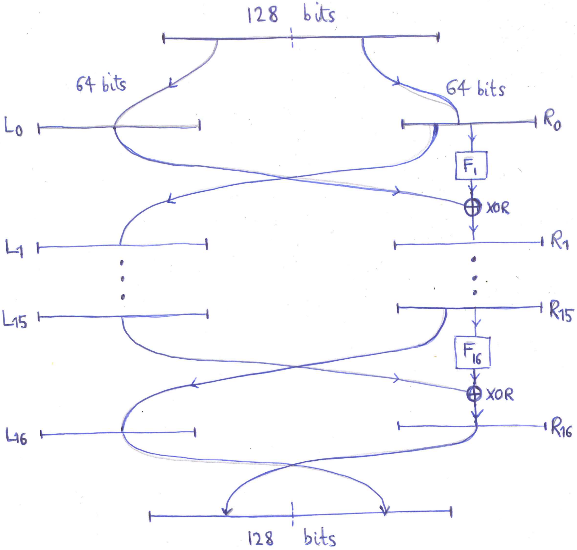
2. 16 rounds of encryption / decryption

Materials: github.com/JoshuaBlinkhorn/Kryptologie-LAB

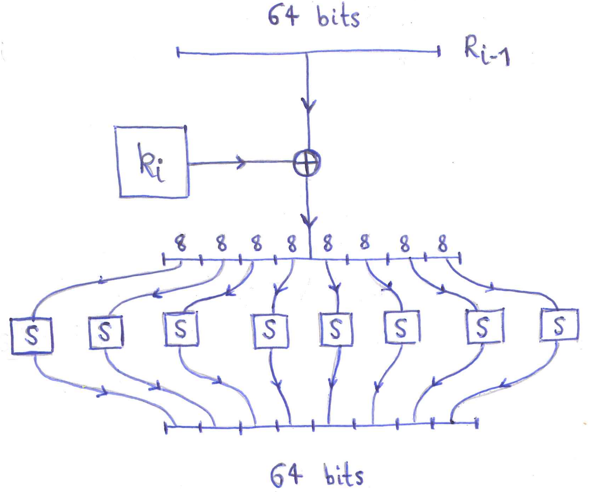
Task 3 - part 2

- Implement data encryption and decryption routines for DES.
    - block cypher with block length 128 bits
    - key length: 64 bits
    - to decrypt, use encryption routine with keys in reverse order
- Use binary data

DES overview



The function F_i



S-box details (1)

- We use only a single S-box
- The S-box defines a lookup table
- A value of $0 \leq x \leq 255$ is substitued by the value $S[x]$
- Text version in the git repository

S-box details (2)

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