Kryptologie LAB - 3.1

Summer Semester 2020

Dr. Joshua Blinkhorn

Friedrich-Schiller-Universität Jena

Data Encryption Standard (DES)

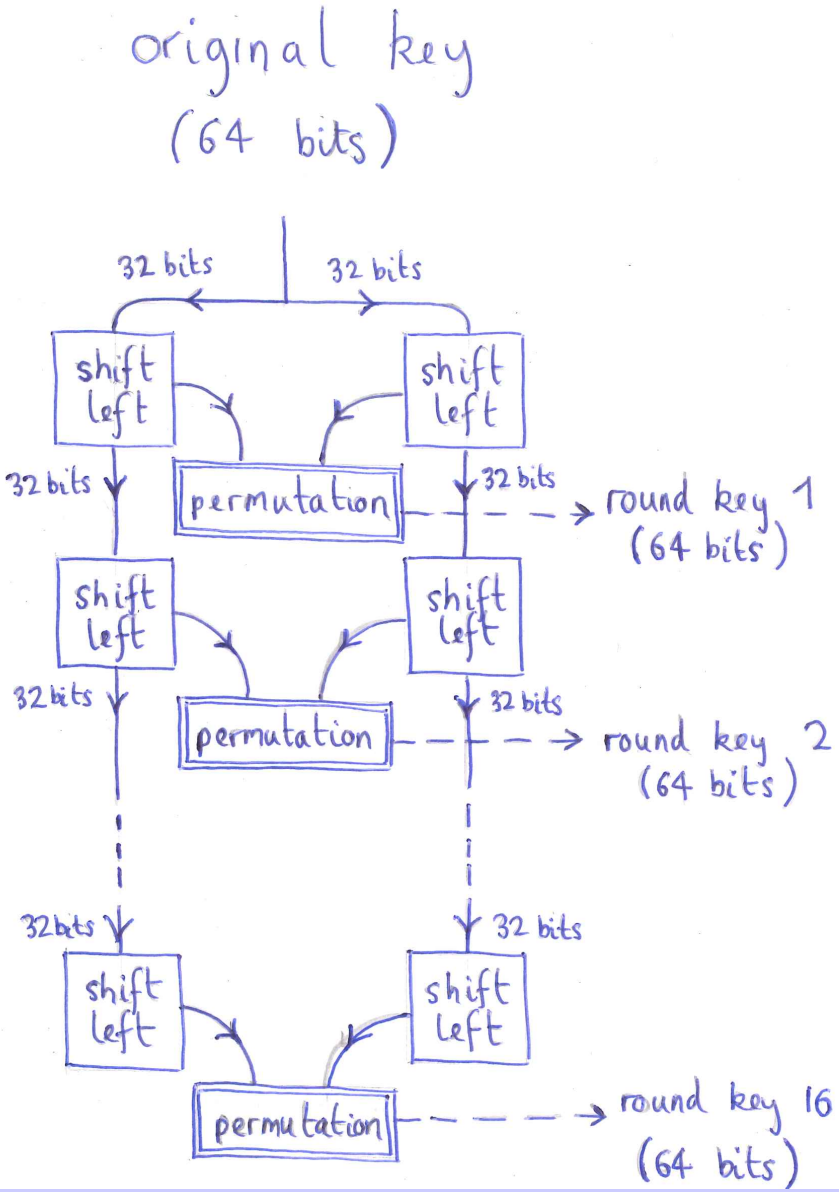
1. Key generation - 16 keys from one key
2. 16 rounds of encryption / decryption

Materials: github.com/JoshuaBlinkhorn/Kryptologie-LAB

Task 3 - part 1

- Implement a key generation routine for DES.
  - the routine generates 16 round keys from the original key
  - key length: 64 bits
  - composed of ‘left shifting’ and a 64-bit permutation
- Use binary data

Key generation overview



Key generation details

- Shift left by 2 bits each round.
- Use the following permutation $\mathbb{Z}_{64} \to \mathbb{Z}_{64}$ to permute bit positions (read along rows first)
- Text version in the git repository

39	46	57	29	50	36	14	8
45	31	53	21	56	55	32	30
16	38	47	37	7	5	27	49
48	58	26	42	60	23	12	44
24	17	6	54	2	34	62	35
22	15	4	43	40	11	51	52
1	33	28	61	18	13	59	19
0	41	20	10	3	9	25	63