Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Homework Sheet 6
Version 02.07.2020

Homework 1.

Calculate the first round key K^1 of the master key $K = \texttt{13 34 57 79 9B BC DF F1}$.

Homework 2.

We consider the DES round key $\tilde{K} \in \mathbb{Z}_2^{48}$ and the text block $X \in \mathbb{Z}_2^{32}$ given by

$$\tilde{K} := \texttt{CC CC 33 33 CC CC} \qquad X := \texttt{00 CC 00 33}.$$

Compute the associated cipher text $E_{\tilde{K}}(X)$ of the inner block cipher associated with the Feistel cipher of the DES.

Homework 3.

Compute all DES master keys of the form

$$\begin{bmatrix} * & * & * & 0 & 1 & 1 & 1 & * \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ * & * & * & 0 & 0 & 0 & 0 & * \\ * & * & * & * & 0 & 0 & 0 & * \\ 1 & * & 1 & 1 & 0 & 0 & 1 & * \\ 1 & 1 & * & 1 & 0 & 1 & 1 & * \\ * & * & * & * & 1 & 1 & 1 & * \end{bmatrix}$$

which generate at most 7 different round keys. Verify correctness of your solution.

Homework 4.

Let $p := 5$ and $q := 7$. Find all involutoric public keys of the associated RSA algorithm, i.e., identify all those encryption coefficients which coincide with their associated decryption coefficients.

Homework 5.

Let $p := 5$, $q := 11$, as well as $n := pq$ and consider the associated RSA algorithm with encryption coefficient $e := 7$. Noting that $0, 1, 54 \in \mathbb{Z}_{55}$ are fixed points of the associated RSA algorithm, we investigate the following plain text alphabet $\mathcal{A} := \{z_i \,|\, i \in \{2, \ldots, 53\}\}$ for encryption via the RSA:

i	z_i	i	z_i	i	z_i	i	z_i
2	a	15	n	28	A	41	N
3	b	16	o	29	B	42	O
4	c	17	p	30	C	43	P
5	d	18	q	31	D	44	Q
6	e	19	r	32	E	45	R
7	f	20	s	33	F	46	S
8	g	21	t	34	G	47	T
9	h	22	u	35	H	48	U
10	i	23	v	36	I	49	V
11	j	24	w	37	J	50	W
12	k	25	x	38	K	51	X
13	l	26	y	39	L	52	Y
14	m	27	z	40	M	53	Z

Decrypt the cipher text `Xtos` which has been created with the aid of this RSA algorithm.

Homework 6.

Factorize 299 using Pollard's $p-1$ method with $\sigma = 5$.