Review Exercise in Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-08-04

Problem 1. Consider the following ciphertext[1] $\tilde{\boldsymbol{c}} = (\tilde{c}_1, \ldots, \tilde{c}_{20})$. Characters are identified by numbers from $\mathbb{Z}_{26} = \{0, \ldots, 25\}$ below:

E	C	T	K	X	E	G	Z	Z	C	D	G	Z	O	D	W	P	E	F	C
4	2	19	10	23	4	6	25	25	2	3	6	25	14	3	22	15	4	5	2

a) Compute the index of coincidence $I_{\tilde{c}}$ for ciphertext $\tilde{\boldsymbol{c}}$.

b) Compute the cardinality of the multiplicative group $|\mathbb{Z}_{26}^*|$.

c) Determine all elements of $\mathbb{Z}_{26}^*$ and determine all inverses[2] in $\mathbb{Z}_{26}^*$.

A combined version of the affine cipher and the Hill cipher was applied for the encryption. The cryptosystem operates on blocks of two symbols each. The plaintext of each block is a vector of two symbols $\boldsymbol{m} = (m_1, m_2)^{\mathrm{T}}$, with each $m_i \in \mathbb{Z}_{26}$. Likewise, the ciphertext of each block is a vector of two symbols $\boldsymbol{c} = (c_1, c_2)^{\mathrm{T}}$, $c_i \in \mathbb{Z}_{26}$. The key block is a tuple $(\boldsymbol{U}, \boldsymbol{a})$ with a matrix $\boldsymbol{U} \in \mathbb{Z}_{26}^{2\times 2}$ and a vector of two symbols $\boldsymbol{a} = (a_1, a_2)^{\mathrm{T}}$, $a_i \in \mathbb{Z}_{26}$. The encryption function e is defined by:

$$e(\boldsymbol{m}) = \boldsymbol{c} = \boldsymbol{U}\boldsymbol{m} + \boldsymbol{a}. \tag{1}$$

d) Give a reason why an inverse matrix of $\boldsymbol{U}$ modulo 26 exists only if $\det(\boldsymbol{U}) \in \mathbb{Z}_{26}^*$ holds.

e) Determine the decryption function d for the given cryptosystem in terms of $\boldsymbol{U}$, $\boldsymbol{m}$, $\boldsymbol{c}$ and $\boldsymbol{a}$.

Oscar has intercepted the key that was used for the encryption of the ciphertext $\tilde{\boldsymbol{c}}$:

$$(\boldsymbol{U} = \begin{pmatrix} 5 & 4 \\ 13 & 7 \end{pmatrix}, \ \boldsymbol{a} = \begin{pmatrix} 11 \\ 18 \end{pmatrix}). \tag{2}$$

f) Compute the inverse matrix of $\boldsymbol{U}$ modulo 26.

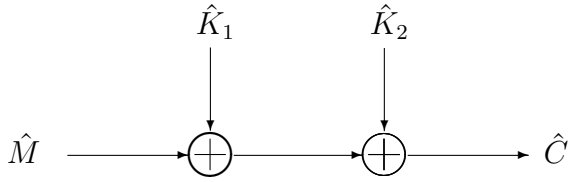
To decipher $\tilde{\boldsymbol{c}}$, the decryption is performed block-wise for blocks of two ciphertext symbols.

g) Decrypt the first six symbols of the given ciphertext $\tilde{\boldsymbol{c}}$.

[1] **Hint:** The plaintext is an English text.

[2] **Hint**: Note that $7 \cdot 15 - 4 \cdot 26 = 1$, $17 \cdot 23 - 15 \cdot 26 = 1$, and $11 \cdot 19 - 8 \cdot 26 = 1$.

Problem 2. In the encryption system depicted above, the message $\hat{M} \in \mathcal{M}$ and



the two keys $\hat{K}_1 \in \mathcal{K}_1$ and $\hat{K}_2 \in \mathcal{K}_2$ are discrete random variables with finite support $\mathcal{M} = \mathcal{K}_1 = \mathcal{K}_2 = \{0, 1\}$. Addition is taken modulo 2. The distributions of the message $\hat{M}$, the key $\hat{K}_1$ and the key $\hat{K}_2$ are given by:

$$P(\hat{M} = 0) = p,\ P(\hat{M} = 1) = 1 - p,\ 0 \leq p \leq 1,$$

$$P(\hat{K}_1 = 0) = q,\ P(\hat{K}_1 = 1) = 1 - q,\ 0 < q < \tfrac{1}{2},$$

$$P(\hat{K}_2 = 0) = r,\ P(\hat{K}_2 = 1) = 1 - r,\ 0 \leq r \leq 1.$$

$\hat{M}$, $\hat{K}_1$, and $\hat{K}_2$ are stochastically independent. Use the dual logarithm in your calculations.

(a) Derive the distribution of $\hat{K}_1 \oplus \hat{K}_2$ in terms of q and r.

(b) Derive the distribution of $\hat{C}$ in terms of p, q and r.

(c) Assume $r = \frac{1}{2}$. Show that the system has perfect secrecy.

(d) Assume $p = \frac{1}{2}$ and $r = \frac{1}{2}$. Show that the message equivocation $H(\hat{M}|\hat{C})$ is greater than the key equivocation $H(\hat{K}_1|\hat{C})$.

Problem 3. Consider the following AES-128 round key K_0 given in hexadecimal notation:

$$K_0 = B8\ 2E\ E1\ 22\ 53\ 1C\ 2D\ 94\ 82\ 1A\ C7\ 55\ BC\ BC\ 58\ 58.$$

Calculate W_4 using Algorithm 1 for the AES key expansion. AES-128 has $r = 10$ rounds.

Algorithm 1 AES key expansion

```
Split K into 4 32-bit words W_0, W_1, W_2, W_3
for (i ← 4; i < 4 · (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
```

The lookup-table for the `SubBytes`-operation of AES is given as:

Further functions are:

- `RotByte` is a cyclic leftshift by one byte

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

- $\texttt{Rcon}(i) = (\texttt{RC}(i), \texttt{00}, \texttt{00}, \texttt{00})$ in hexadecimal notation
- $\texttt{RC}(i)$ represents x^{i-1} as element of $\mathbb{F}_{2^8}$ in polynomial notation

Problem 4.

a) Formulate the Diffie-Hellman key agreement protocol based on the discrete logarithm.

b) Use the Miller-Rabin Primality Test to show that $a = 2$ is not a strong witness for the compositeness of $p = 37$.

c) The public parameters for the DHP are set to $p = 37$ and $a = 5$. Check if these are valid parameters for the DHP. Alice chooses $x = 8$, Bob chooses $y = 16$. Perform the DHP with the above parameters.

Problem 5. We now consider the RSA-cryptosystem.

a) Alive uses the public key $(n, e) = (221, 5)$. Decrypt the ciphertext $c = 9$. Begin with factoring n.

b) How many RSA keys exist for two given primes p and q?