Review Exercise in Cryptography
- Proposed Solution -

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

2015-08-04

Solution of Problem 1

a) With $n = 20$ and the frequency analysis:

ℓ	C	D	E	F	G	K	O	P	T	W	X	Z
N_ℓ	3	2	3	1	2	1	1	1	1	1	1	3

, **(1P)**

we can calculate the index of coincidence for $\tilde{\boldsymbol{c}}$:

$$I_{\tilde{\boldsymbol{c}}} = \sum_{\ell=0}^{25} \frac{N_\ell(N_\ell - 1)}{n(n-1)} = \frac{3 \cdot 3 \cdot 2 + 2 \cdot 2 \cdot 1}{20 \cdot 19} = \frac{18+4}{380} = \frac{22}{380} = \frac{11}{190} \approx 0.0579\,. \textbf{ (2P)}$$

b) With $gcd(13, 2) = 1$, 13 prime and 2 prime:

$$|\mathbb{Z}_{26}^*| = \varphi(26) = \varphi(13 \cdot 2) = \varphi(13) \cdot \varphi(2) = (13-1) \cdot (2-1) = 12 \textbf{ (2P)}$$

c) Exclude all numbers that, without remainder, divide prime factors of $26 = 13 \cdot 2$, i.e., exclude all even numbers, and also 13:

$$|\mathbb{Z}_{26}^*| = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \textbf{ (1P)}$$

The inverses are:

$$\begin{aligned}
1^{-1} &\equiv 1 \mod 26 \\
3^{-1} &\equiv 9 \mod 26, \text{ since } 3 \cdot 9 \equiv 1 \mod 26 \\
5^{-1} &\equiv 21 \mod 26, \text{ since } 5 \cdot (-5) \equiv -25 \equiv -1 \mod 26 \\
7^{-1} &\equiv 15 \mod 26, \text{ by hint} \\
9^{-1} &\equiv 3 \mod 26, \text{ by symmetry} \\
11^{-1} &\equiv 19 \mod 26, \text{ by hint} \\
15^{-1} &\equiv 7 \mod 26, \text{ by symmetry} \\
17^{-1} &\equiv 23 \mod 26, \text{ by hint} \\
19^{-1} &\equiv 11 \mod 26, \text{ by symmetry} \\
21^{-1} &\equiv 5 \mod 26, \text{ by symmetry} \\
23^{-1} &\equiv 17 \mod 26, \text{ by symmetry} \\
25^{-1} &\equiv 25 \mod 26, \text{ since } 25 \equiv -1 \mod 26 \text{ and } (-1) \cdot (-1) \equiv 1 \mod 26
\end{aligned}$$

$3^{-1}, 1^{-1}, 5^{-1}, 25^{-1}$ **(3P)**
$9^{-1}, 21^{-1}, 7^{-1}, 11^{-1}, 17^{-1}, 23^{-1}, 19^{-1}, 15^{-1}$ **(2P)**

d) $\boldsymbol{U}$ is invertible in $\mathbb{Z}_{26}$ if $\boldsymbol{U}\boldsymbol{U}^{-1} \equiv \boldsymbol{I} \mod 26$.

It holds that $\det(\boldsymbol{I}) = \det(\boldsymbol{U}\boldsymbol{U}^{-1}) \equiv \det(\boldsymbol{U}) \cdot \det(\boldsymbol{U}^{-1}) \equiv 1$.

Let $\det(\boldsymbol{U}) = a \mod 26 \Rightarrow \det(\boldsymbol{U}^{-1}) = a^{-1} \mod 26$.

The inverse a^{-1} exists only if $a \in \mathbb{Z}_{26}^*$. **(3P)**

Alternative solution:
In $\mathbb{Z}_{26}$, a unique inverse

$$\boldsymbol{U}^{-1} \equiv \det(\boldsymbol{U})^{-1} \begin{pmatrix} u_{22} & -u_{12} \\ -u_{21} & u_{11} \end{pmatrix} \pmod{26}$$

only exists, if $\det(\boldsymbol{U})^{-1}$ is invertible mod 26, i.e., if $\det(\boldsymbol{U})^{-1} \in \mathbb{Z}_{26}^*$.

e) $d(\boldsymbol{c}) = \boldsymbol{m} = \boldsymbol{U}^{-1}(\boldsymbol{c} - \boldsymbol{a})$ **(1P)**

f) $\det(\boldsymbol{U}) = 5 \cdot 7 - 4 \cdot 13 = -17 \equiv 9\,,\ 9 \in \mathbb{Z}_{26}^* \Rightarrow \boldsymbol{U}^{-1} \mod 26$ exists. **(1P)**

$$\begin{aligned}
\boldsymbol{U}^{-1} &= \det(\boldsymbol{U})^{-1} \cdot \begin{pmatrix} u_{22} & -u_{12} \\ -u_{21} & u_{11} \end{pmatrix} \\
&= 9^{-1} \cdot \begin{pmatrix} 7 & -4 \\ -13 & 5 \end{pmatrix} \\
&\overset{(c)}{\equiv} 3 \cdot \begin{pmatrix} 7 & 22 \\ 13 & 5 \end{pmatrix} \\
&= \begin{pmatrix} 21 & 66 \\ 39 & 15 \end{pmatrix} \\
&\equiv \begin{pmatrix} 21 & 14 \\ 13 & 15 \end{pmatrix} \mod 26 \ \textbf{(3P)}
\end{aligned}$$

An alternative solution via Gauss elimination:

5	4	1	0	$\mid \cdot 21$
13	7	0	1	
1	6	21	0	$\mid \cdot (-13)$
13	7	0	1	
−13	0	−13	0	$\downarrow (+)$
13	7	0	1	
1	6	21	0	
0	7	−13	1	$\mid \cdot (-5)$
1	6	21	0	
0	−1	13	−15	$\mid \cdot 6 \uparrow (+)$
1	0	21	14	
0	1	13	15	

// Validity check:

$$\boldsymbol{U}\boldsymbol{U}^{-1} \equiv \begin{pmatrix} 5 & 4 \\ 13 & 7 \end{pmatrix} \cdot \begin{pmatrix} 21 & 14 \\ 13 & 15 \end{pmatrix} = \begin{pmatrix} 157 & 130 \\ 364 & 287 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv \boldsymbol{I} \mod 26 \ \checkmark$$

g)

$$\boldsymbol{m} = \boldsymbol{U}^{-1}(\boldsymbol{c} - \boldsymbol{a}) \mod 26$$

$$\begin{pmatrix}21 & 14\\13 & 15\end{pmatrix}\begin{pmatrix}4-11\\2-18\end{pmatrix} = \begin{pmatrix}539\\397\end{pmatrix} \equiv \begin{pmatrix}19\\7\end{pmatrix} \mod 26 \to \begin{pmatrix}T\\H\end{pmatrix}$$
$$\begin{pmatrix}21 & 14\\13 & 15\end{pmatrix}\begin{pmatrix}19-11\\10-18\end{pmatrix} = \begin{pmatrix}420\\374\end{pmatrix} \equiv \begin{pmatrix}4\\10\end{pmatrix} \mod 26 \to \begin{pmatrix}E\\K\end{pmatrix}$$
$$\begin{pmatrix}21 & 14\\13 & 15\end{pmatrix}\begin{pmatrix}23-4\\4-18\end{pmatrix} = \begin{pmatrix}420\\336\end{pmatrix} \equiv \begin{pmatrix}4\\24\end{pmatrix} \mod 26 \to \begin{pmatrix}E\\Y\end{pmatrix}$$ **(3P)**

// Just for the sake of completeness, we provide the rest of the plaintext:

$$\begin{pmatrix}21 & 14\\13 & 15\end{pmatrix}\begin{pmatrix}4-11\\2-18\end{pmatrix} = \begin{pmatrix}539\\397\end{pmatrix} \equiv \begin{pmatrix}19\\7\end{pmatrix} \mod 26 \to \begin{pmatrix}T\\O\end{pmatrix}$$
$$\begin{pmatrix}21 & 14\\13 & 15\end{pmatrix}\begin{pmatrix}19-11\\10-18\end{pmatrix} = \begin{pmatrix}420\\374\end{pmatrix} \equiv \begin{pmatrix}4\\10\end{pmatrix} \mod 26 \to \begin{pmatrix}S\\U\end{pmatrix}$$
$$\begin{pmatrix}21 & 14\\13 & 15\end{pmatrix}\begin{pmatrix}23-4\\4-18\end{pmatrix} = \begin{pmatrix}420\\336\end{pmatrix} \equiv \begin{pmatrix}4\\24\end{pmatrix} \mod 26 \to \begin{pmatrix}C\\C\end{pmatrix}$$
$$\begin{pmatrix}21 & 14\\13 & 15\end{pmatrix}\begin{pmatrix}4-11\\2-18\end{pmatrix} = \begin{pmatrix}539\\397\end{pmatrix} \equiv \begin{pmatrix}19\\7\end{pmatrix} \mod 26 \to \begin{pmatrix}E\\S\end{pmatrix}$$
$$\begin{pmatrix}21 & 14\\13 & 15\end{pmatrix}\begin{pmatrix}19-11\\10-18\end{pmatrix} = \begin{pmatrix}420\\374\end{pmatrix} \equiv \begin{pmatrix}4\\10\end{pmatrix} \mod 26 \to \begin{pmatrix}S\\I\end{pmatrix}$$
$$\begin{pmatrix}21 & 14\\13 & 15\end{pmatrix}\begin{pmatrix}23-4\\4-18\end{pmatrix} = \begin{pmatrix}420\\336\end{pmatrix} \equiv \begin{pmatrix}4\\24\end{pmatrix} \mod 26 \to \begin{pmatrix}S\\Y\end{pmatrix}$$
$$\begin{pmatrix}21 & 14\\13 & 15\end{pmatrix}\begin{pmatrix}23-4\\4-18\end{pmatrix} = \begin{pmatrix}420\\336\end{pmatrix} \equiv \begin{pmatrix}4\\24\end{pmatrix} \mod 26 \to \begin{pmatrix}O\\U\end{pmatrix}$$

Solution of Problem 2

a)

$$\begin{aligned}P(K_1 \oplus K_2 = 0) &= P(K_1 = 0) \cdot P(K_2 = 0) + P(K_1 = 1) \cdot P(K_2 = 1)\\ &= q \cdot r + (1-q) \cdot (1-r)\\ &= 1 - q - r + 2qr\\ &= s.\end{aligned}$$

$$\begin{aligned}P(K_1 \oplus K_2 = 1) &= P(K_1 = 0) \cdot P(K_2 = 1) + P(K_1 = 1) \cdot P(K_2 = 0)\\ &= q \cdot (1-r) + (1-q) \cdot r\\ &= q + r - 2qr\\ &= 1 - s.\end{aligned}$$ **(4P)**

b) $K_1 \oplus K_2 = K$
$P(C) = P(M \oplus K_1 \oplus K_2) = P(M \oplus K)$

$$\begin{aligned} P(C=0) = P(M \oplus K = 0) &= P(M=0) \cdot P(K=0) + P(M=1) \cdot P(K=1) \\ &= p \cdot s + (1-p) \cdot (1-s) \\ &= p + q + r - 2qr - 2pq - 2pr + 4pqr. \end{aligned}$$

$$\begin{aligned} P(C=1) = P(M \oplus K = 1) &= P(M=0) \cdot P(K=1) + P(M=1) \cdot P(K=0) \\ &= p \cdot (1-s) + (1-p) \cdot s \\ &= 1 - p - q - r + 2qr + 2pq + 2pr - 4pqr. \ \textbf{(4P)} \end{aligned}$$

c) Perfect secrecy $\Leftrightarrow H(M \mid C) = H(M)$
$r = \frac{1}{2} \Rightarrow P(K=0) = 1 - q - \frac{1}{2} + 2q\frac{1}{2} = \frac{1}{2}$
$r = \frac{1}{2} \Rightarrow P(K=1) = \frac{1}{2} + q - 2q\frac{1}{2} = \frac{1}{2}$
$\Rightarrow H(K) = 1.$

$r = \frac{1}{2} \Rightarrow P(C=0) = p + q + \frac{1}{2} - 2q\frac{1}{2} - 2pq - 2p\frac{1}{2} + 4pq\frac{1}{2} = \frac{1}{2}$
$r = \frac{1}{2} \Rightarrow P(C=1) = 1 - p - q - \frac{1}{2} + 2q\frac{1}{2} + 2pq + 2p\frac{1}{2} - 4pq\frac{1}{2} = \frac{1}{2}$
$\Rightarrow H(C) = 1.$

$$\begin{aligned} H(M \mid C) &= H(M, C) - H(C) \\ &= H(C \mid M) + H(M) - H(C) \\ &= H((M \oplus K) \mid M) + H(M) - H(C) \\ &= H(K) + H(M) - H(C) \\ &= H(M). \ \textbf{(5P)} \end{aligned}$$

d) $H(M \mid C) = H(K) + H(M) - H(C)$
$p = \frac{1}{2} \Rightarrow H(M) = 1$
$r = \frac{1}{2} \Rightarrow H(K) = H(C) = 1$
$\Rightarrow H(M \mid C) = 1$

$$\begin{aligned} H(K_1 \mid C) &= H(K_1, C) - H(C) \\ &= H(C \mid K_1) + H(K_1) - H(C) \\ &= H((M \oplus K_1 \oplus K_2) \mid K_1) + H(K_1) - H(C) \\ &= H(M \oplus K_2) + H(K_1) - H(C). \end{aligned}$$

$p = \frac{1}{2} \Rightarrow H(M \oplus K_2) = 1$
$r = \frac{1}{2} \Rightarrow H(K) = H(C) = 1$
$\Rightarrow H(K_1 \mid C) = H(K_1) < 1$

$\Rightarrow H(K_1 \mid C) < H(M \mid C).$ **(4P)**

Solution of Problem 3

The given AES-128 round key is denoted in hexadecimal representation:

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

- The round key is $K_0 = K = (W_0\ W_1\ W_2\ W_3)$ with $W_0 = (B8\ 2E\ E1\ 22)$, $W_1 = (53\ 1C\ 2D\ 94)$, $W_2 = (82\ 1A\ C7\ 55)$, $W_3 = (BC\ BC\ 58\ 58)$.
- To calculate W_4 and W_5 (the first 8 bytes of round key K_1) use Alg. 1 for the AES key expansion and recall that $K_1 = (W_4\ W_5\ W_6\ W_7)$.

Algorithm 1 AES key expansion (applied)

for $i \leftarrow 4;\ i < 4 \cdot (r+1);\ i{+}{+}$ **do**
  \\ Initialize for-loop with $i \leftarrow 4$. We have $r = 1$ for K_1.
  tmp $\leftarrow W_{i-1}$
  \\ tmp $\leftarrow W_3 = (BC\ BC\ 58\ 58)$ **(1P)**
  if $(i \mod 4 = 0)$ **then**
    \\ Result is *true* as $i = 4$.
    tmp $\leftarrow$ `SubBytes`(`RotByte`(tmp)) $\oplus$ `Rcon`$(i/4)$
    \\ Evaluate this operation step by step:
    \\ `RotByte`(tmp) $= (BC\ 58\ 58\ BC)$, i.e., a cyclic left shift of one byte **(2P)**
    \\ To compute `SubBytes`$(BC\ 58\ 58\ BC)$ use given lookup-table for each byte:
    \\ (row 11, col 12) provides $101_{10} = 65_{16}$
    \\ (row 5, col 8) provides $106_{10} = 6A_{16}$
    \\ Note that the indexation of rows and columns starts with zero.
    \\ `SubBytes`$(BC\ 58\ 58\ BC) = (65\ 6A\ 6A\ 65)$ **(3P)**
    \\ $i/4 = 1$
    \\ `Rcon`$(1) =$ (`RC`(1) 00 00 00), with `RC`$(1) = x^{1-1} = x^0 = 1 \in \mathbb{F}_{2^8}$.
    \\ tmp $\leftarrow (65\ 6A\ 6A\ 65) \oplus (01\ 00\ 00\ 00) = (64\ 6A\ 6A\ 65)$ **(2P)**
  end if
  $W_i \leftarrow W_{i-4} \oplus$ tmp \\ $W_4 \leftarrow W_0 \oplus$ tmp. Then, next iteration, $i \leftarrow 5$...
end for

	W_0	B	8	2	E	E	1	2	2
$\oplus$	tmp	6	B	6	5	6	5	6	A
	W_0	1011	1000	0010	1110	1110	0001	0010	0010
$\oplus$	tmp	0110	0100	0110	1010	0110	1010	0110	0101
	W_4	1101	1100	0100	0100	1000	1011	0100	0111
	W_4	D	C	4	4	8	B	4	7

(3P)

Solution of Problem 4

a) **Initial setup:**

A prime p and a primitive element a modulo p are selected and published.

Protocol actions:

A chooses a random secret $x \in \{2, \ldots, p-2\}$ and sends to B: $u = a^x \mod p$.
B chooses a random secret $y \in \{2, \ldots, p-2\}$ and sends to A: $v = a^y \mod p$.
B receives u and computes the shared key $u^y = (a^x)^y \mod p$.
A receives v and computes the shared key $v^x = (a^y)^x \mod p$.

(2P)

b) Apply the MRPT, compute q and k:

$$\begin{aligned} p = 37 &= 1 + q \cdot 2^k \\ &= 1 + 18 \cdot 2^1 \\ &= 1 + 9 \cdot 2^2 \quad \Rightarrow \quad q = 9\,,\, k = 2 \end{aligned}$$ **(1P)**

The witness is chosen as $a = 2$, and we have $k = 2$:

$$\begin{aligned} &y \leftarrow a^q = 2^9 = 512 \equiv 31 \mod 37 \\ &y \not\equiv 1 \mod 37, \quad y \not\equiv 36 \mod 37 \\ &i = 1 : y \leftarrow a^{q \cdot 2^i} = y^2 = 31^2 = 961 \equiv 36 \equiv -1 \mod 37 \\ &\Rightarrow \text{The MRPT states } n = 37 \text{ is prime.} \end{aligned}$$ **(3P)**

c) The parameters are valid if $p = 37$ is prime and $a = 5$ is a primitive element.
From (b), we assume that $p = 37$ is prime. **(1P)**
Is $a = 5$ a primitive element? From Proposition 7.5 it follows:

$$a \text{ is a primitive element modulo } p \iff a^{(p-1)/p_i} \not\equiv 1 \pmod{p} \quad \forall i = 1, \ldots, k.$$

$$p = 37\,,\, p - 1 = 37 - 1 = 36 \quad p_1 = 2, p_2 = 3 \quad 36 = 2^2 \cdot 3^2$$

$$a^{\frac{p-1}{p_1}} = 5^{\frac{36}{2}} = 5^{18} \equiv 36 \not\equiv 1 \mod 37$$

$$a^{\frac{p-1}{p_2}} = 5^{\frac{36}{3}} = 5^{12} = 244140625 \equiv 10 \not\equiv 1 \mod 37$$

$\Rightarrow a$ is a primitive element and the parameters are valid. **(2P)**

$$\begin{aligned} a^x &= 5^8 = 390625 \equiv 16 \mod 37 \\ (a^x)^y &= 16^{16} = 16^{8 \cdot 2} = 4294967296^2 \equiv 7^2 \equiv 12 \mod 37 \\ a^y &= 5^{16} = \left(5^8\right)^2 = 16^2 \equiv 34 \mod 37 \\ (a^y)^x &= 34^8 = \left(34^4\right)^2 = 1336336^2 \equiv 7^2 \equiv 12 \mod 37 \end{aligned}$$ **(3P)**

Solution of Problem 5

a) $(n, e) = (221, 5)$, $c = 9$

$$\begin{aligned} n &= 221 = 17 \cdot 13 \\ \varphi(n) &= 16 \cdot 12 = 192 \\ d &= e^{-1} = 5^{-1} \mod \varphi(n) \end{aligned}$$ **(1P)**

Extended Euclidean Algorithm:

$$\begin{aligned} 192 &= 5 \cdot 38 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ \Rightarrow 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (192 - 5 \cdot 38) \\ &= 5 - 2 \cdot 192 + 76 \cdot 5 \\ &= 77 \cdot 5 - 2 \cdot 192 \\ \Rightarrow d &= e^{-1} = 77 \mod 192 \\ m &= c^d = 9^{77} \mod 221 \end{aligned}$$ **(2P)**

Decimal to binary representation of 77:

$$\begin{aligned} 77 &= 2 \cdot 38 + 1 && 2^0 \\ 38 &= 2 \cdot 19 + 0 && 2^1 \\ 19 &= 2 \cdot 9 + 1 && 2^2 \\ 9 &= 2 \cdot 4 + 1 && 2^3 \\ 4 &= 2 \cdot 2 + 0 && 2^4 \\ 2 &= 2 \cdot 1 + 0 && 2^5 \\ 1 &= 2 \cdot 0 + 1 && 2^6 \\ \Rightarrow 77_{10} &= 1001101_2 \end{aligned}$$ **(1P)**

Square and Multiply:

$$\begin{aligned} &9 \\ 9^2 &\equiv 81 \mod 221 \\ 81^2 &\equiv 152 \mod 221 \\ 152^2 \cdot 9 &\equiv 196 \mod 221 \\ 196^2 \cdot 9 &\equiv 100 \mod 221 \\ 100^2 &\equiv 55 \mod 221 \\ 55^2 \cdot 9 &\equiv 42 \equiv 9^{77} \mod 221 \end{aligned}$$ **(2P)**

b) Key is generated such that:

$$d = e^{-1} \mod \varphi(n)\,.$$

$\Rightarrow$ There are $\varphi(\varphi(n))$ such numbers. **(2P)**