**Prof. Dr. Rudolf Mathar, Dr. Michael Reyer**

# Tutorial 13
# - Proposed Solution -

Friday, July 26, 2019

## Solution of Problem 1

**a)** With $n = 39$ and frequency analysis

| $\ell$ | A | B | E | F | G | H | L | N | P | R | S | U | V | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $N_\ell$ | 5 | 5 | 3 | 2 | 5 | 2 | 1 | 2 | 1 | 3 | 2 | 1 | 5 | 1 | 1 |

we can calculate the index of coincidence as

$$I_C = \sum_{\ell=0}^{25} \frac{N_\ell(N_\ell - 1)}{n(n-1)} = \frac{4 \cdot (2 \cdot 1) + 2 \cdot (3 \cdot 2) + 4 \cdot (5 \cdot 4)}{39 \cdot 38} = \frac{100}{1482} \approx 0.06748$$

**b)** $I_C$ is close to $\kappa_E = 0.0669$, so it is likely that a monoalphabetic cipher was used.

**c)** From the first four letters, we can see that the Caesar cipher with a rotation of 13 was used. The plain text is calculated as follows.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Y | V | I | R | Y | B | A | T | N | A | Q | C | E | B | F | C | R | E |
| 24 | 21 | 8 | 17 | 24 | 1 | 0 | 19 | 13 | 0 | 16 | 2 | 4 | 1 | 5 | 2 | 17 | 4 |
| L | I | V | E | L | O | N | G | A | N | D | P | R | O | S | P | E | R |
| 11 | 8 | 21 | 4 | 11 | 14 | 13 | 6 | 0 | 13 | 3 | 15 | 17 | 14 | 18 | 15 | 4 | 17 |

**d)** Some types of attacks are as follows.

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack

**e)** $\boldsymbol{P} \in \{0,1\}^{k \times k}$. The sum of each row (and column) needs to be one for $\boldsymbol{P}$ to be a permutation matrix.

**f)** Using some public initial vector $\boldsymbol{c}_0$ the cryptograms for $n \in \mathbb{N}$ are calculated as

$$\boldsymbol{c}_n = e(\boldsymbol{m}_n \oplus \boldsymbol{c}_{n-1}) = (\boldsymbol{m}_n \oplus \boldsymbol{c}_{n-1})\boldsymbol{P}.$$

## Solution of Problem 2

**a)** It holds

$$H(\hat{C} \mid \hat{M}) = \sum_{M \in \mathcal{M}} P(\hat{M} = M) H(\hat{C} \mid \hat{M} = M).$$

Calculate

$$\begin{aligned} H(\hat{C} \mid \hat{M} = M) &= -\sum_{C \in \mathcal{C}} P(\hat{C} = C \mid \hat{M} = M) \log P(\hat{C} = C \mid \hat{M} = M) \\ &= -(1-\epsilon)\log(1-\epsilon) - 3\frac{\epsilon}{3}\log\left(\frac{\epsilon}{3}\right) = -(1-\epsilon)\log(1-\epsilon) - \epsilon\log(\epsilon) + \epsilon\log(3) \end{aligned}$$

which is independent of $P(\hat{M} = M)$, and hence

$$H(\hat{C} \mid \hat{M}) = \sum_{M \in \mathcal{M}} P(\hat{M} = M) H(\hat{C} \mid \hat{M} = M) = -(1-\epsilon)\log(1-\epsilon) - \epsilon\log(\epsilon) + \epsilon\log(3).$$

For calculating $P(\hat{C} = C)$ we condition on $\hat{M}$.

$$P(\hat{C} = C) = \sum_{M \in \mathcal{M}} P(\hat{M} = M) P(\hat{C} = C \mid \hat{M} = M) = (1-\epsilon) P(\hat{M} = C) + \frac{\epsilon}{3} P(\hat{M} \neq C).$$

**b)** If $\hat{M}$ is uniformly distributed, then

$$P(\hat{C} = C) = (1-\epsilon)\frac{1}{4} + \frac{\epsilon}{3}\frac{3}{4} = \frac{1}{4},$$

and hence,

$$H(\hat{C}) = \log(4).$$

Moreover, $H(\hat{M}) = \log(4)$ since it is uniformly distributed. From the chainrule in Theorem 4.3 we get
$H(\hat{M}) - H(\hat{M} \mid \hat{C}) = H(\hat{C}) - H(\hat{C} \mid \hat{M})$ which implies that

$$H(\hat{M} \mid \hat{C}) = H(\hat{C} \mid \hat{M}),$$

as $H(\hat{C}) = H(\hat{M})$.

**c)** Using the expression of $H(\hat{M} \mid \hat{C})$ from above, the expression follows.

**d)** The perfect secrecy is achieved when $P(\hat{C} = C \mid \hat{M} = M)$ does not depend on $M$ and $C$. Hence:

$$1 - \epsilon = \frac{\epsilon}{3} \implies \epsilon = \frac{3}{4}.$$

## Solution of Problem 3

**a)** We show that $a = 2$ is a primitve elements utilizing Prop. 7.5

$$a \text{ is PE modulo } p \Leftrightarrow a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p} \ \forall p_i$$

where $p - 1 = \prod_i p_i^{k_i}$ is the prime factorization of $p - 1$.
With $p - 1 = 178 = 2 \cdot 89$ it holds

$$a^2 \equiv 4 \pmod{179},$$

$$a^{89} \equiv ((2^7)^2)^6 \cdot 2^5 \equiv (95^2)^3 \cdot 32 \equiv (75)^2 \cdot 75 \cdot 32 \equiv 76 \cdot 73 \equiv -1 \pmod{179},$$

which verifies the claim.

| Bit | S | M |
|---|---|---|
| 1 | 2 | - |
| 0 | 4 | - |
| 1 | 16 | 32 |
| 1 | 129 | 79 |
| 0 | 155 | - |
| 0 | 39 | - |
| 1 | 89 | 178 |

**b)** First Alice calculates $u = a^{x_A} \mod p$:

$$u = a^{x_A} \equiv 2^{23} = 2^{14} \cdot 2^9 \equiv 95 \cdot 154 \equiv 131 \pmod{179},$$

hence, $u = 131$. Bob equally finds $v = a^{x_B} \mod p$:

$$a^{x_B} \equiv 2^{31} \equiv 2^{23} 2^8 \equiv 131 \cdot 77 \equiv 63 \pmod{179},$$

hence $v = 63$.

| Bit | S | M |
|---|---|---|
| 1 | 2 | - |
| 0 | 4 | - |
| 1 | 16 | 32 |
| 1 | 129 | 79 |
| 1 | 155 | 131 |

| Bit | S | M |
|---|---|---|
| 1 | 2 | - |
| 1 | 4 | 8 |
| 1 | 64 | 128 |
| 1 | 95 | 11 |
| 1 | 121 | 63 |

It holds $31 \cdot 23 \mod p - 1 = 1$, and hence,

$$v^{x_A} \equiv (2^{31})^{23} \equiv 2^1 \equiv 2 \pmod{179}.$$

**c)** Oscar should use $z = 89$. He sends $u^{89} \mod 179$ in place of $u$ to Bob. Oscar sends as well $v^{89} \mod 179$. The shared key will be either $+1$ or $-1$.

**d)** A simple solution would be to exclude $\pm 1$.

## Solution of Problem 4

**a)** $n = p \cdot q = 143$, $\varphi(n) = \varphi(p \cdot q) = (p-1)(q-1) = 10 \cdot 12 = 120$.

$$d = e^{-1} \bmod \varphi(n) = e^{-1} \bmod 120$$

It holds $1 = 1 \cdot 120 - 17 \cdot 7$, and hence, $d = 103$.

$$m = c^d \bmod n = 31^{103} \bmod 143$$

Use square and multiply to calculate $m = 47$.

| Bit | S | M |
|---|---|---|
| 1 | 31 | - |
| 1 | 103 | 47 |
| 0 | 64 | - |
| 0 | 92 | - |
| 1 | 27 | 122 |
| 1 | 12 | 86 |
| 1 | 103 | 47 |

**b)** Keys are generated such that

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

It follows that there are $\varphi(\varphi(n))$ such numbers.

**c)** The public parameters and the received ciphertext are:

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

The plaintext $m$ is not relatively prime to $n$ , i.e., $p \mid m$ or $q \mid m$ and $p \neq q$.

Hence, $\gcd(m, n) \in \{p, q\}$ holds. The $\gcd(m, n)$ can be easily computed such that both primes can be calculated by either $q = \frac{n}{p}$ or $p = \frac{n}{q}$.

The private key $d$ can be computed since the factorization of $n = p\,q$ is known.

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

This inverse is computed using the extended Euclidean algorithm.

**d)** Using Euler's criterion, $-1$ is a quadratic residue if and only if $(-1)^{\frac{p-1}{2}} = 1$, which means $\frac{p-1}{2} = 2k$ or equivalently $p = 4k + 1$.