Exercise 2 in Cryptography
- Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo
2015-04-23

Solution of Problem 4

a) Decryption is easy because:
   - The text structure is visible: spaces and punctuation marks are not encrypted, we can guess the grammatical structure of the text, etc.
   - The language of the plaintext is known
   - Some words occur several times in the ciphertext, e.g., “du”, “spip” and “pjiwtxrinxdc” ⇒ monoalphabetic ⇒ ceasar/substitution cipher

b) Assume Caesar cipher and try to decrypt short words with different keys 1, 2, ... until you obtain a meaningful word:
   xh → yi, zj, ak, bl, cm, dn, eo, fp, gq, hr, is
   iwt → jxu, ..., the
   pjiwtcixrinxdc → qjxudjysqjyed,...,authentication
   In all 3 cases, we add 11 to decrypt.

Other suitable candidates for short words are for example “du”, “id”, “ph”, “spip”, or “pcs”. Otherwise, it is reasonable to guess that xh → is from the grammatical structure.

Frequency Analysis:

| A B C D E F G H I J N P R S T U V W X | 3 3 13 10 3 1 7 8 25 6 7 18 9 6 13 4 3 7 18 |

Check ETAOIN: I → T, P → A, X → I, C → N, T → E, D → O

Letters IPXCTD comprise \( \frac{97}{164} \approx 59\% \) of the ciphertext.

It follows that the Caesar cipher is used with the (secret) encryption key:

\[ k = -11 \equiv 15 \mod 26 \]

Decryption is performed by:

\[ d(c_i) = (c_i - k) \mod 26 \]

The plaintext yields: cryptography is the study of mathematical techniques ...

(see Introduction, quotation in the lecture notes).
Solution of Problem 5

a) Prove that: $a \in \mathbb{Z}_m$ is invertible $\iff \gcd(a, m) = 1$.

"$\Rightarrow$" Show that if $a$ is invertible, then $\gcd(a, m) = 1$. Assume $a^{-1}$ exists:

$$x \equiv a^{-1} \mod m$$

$$\Rightarrow ax \equiv 1 \mod m$$

$$\Rightarrow m \mid (ax - 1)$$

$$\Rightarrow ax - 1 = bm, \quad \exists b \in \mathbb{Z}$$

$$\Rightarrow ax - bm = 1 = n \left( \frac{ax}{n} - \frac{bm}{n} \right), \quad n \in \mathbb{N}$$

$$\Rightarrow n = 1 \Rightarrow \gcd(a, m) = 1 \checkmark$$

"$\Leftarrow$" Show that the inverse $a$ modulo $m$ exists if $\gcd(a, m) = 1$.

$$\gcd(a, m) = 1$$

$$\Rightarrow ax + bm = 1, \quad \exists x, b \in \mathbb{Z} \text{ from the Ext. Euclidean Alg.}$$

$$\Rightarrow ax - 1 = bm$$

$$\Rightarrow m \mid (ax - 1)$$

$$\Rightarrow ax \equiv 1 \mod m$$

$$\Rightarrow x \equiv a^{-1} \mod m \checkmark$$

b) Show that: $\gcd(a, b) = \gcd(b, r)$ holds for the given conditions.

$$\gcd(a, b) = \gcd(bq + r, b) \overset{(1)}{=} \gcd(r, b) = \gcd(b, r).$$

To show (1), set $\gcd(a, b) = d$ and $\gcd(b, r) = e$:

$$d \mid a \land d \mid b \Rightarrow d \mid (a - bq) \Rightarrow d \mid r$$

$$\Rightarrow \text{Since } \gcd(b, r) = e \Rightarrow d \leq e$$

$$e \mid b \land e \mid r \Rightarrow e \mid (bq + r) \Rightarrow e \mid a$$

$$\Rightarrow \text{Since } \gcd(a, b) = d \Rightarrow e \leq d$$

These two properties yield $e = d$.

c) Properties of a multiplicative group with $a, b, c \in \mathbb{Z}_m^*$ are fulfilled:

- Closure (Multiplication):

$$\overset{(aa^{-1})(bb^{-1}) \equiv 1 \mod m}{\Rightarrow (ab)(a^{-1}b^{-1}) \equiv 1 \mod m}$$

$$\Rightarrow (ab)(ab)^{-1} \equiv 1 \mod m$$

$$\Rightarrow (ab)^{-1} \in \mathbb{Z}_m^* \checkmark$$

- Commutativity: $ab = ba \in \mathbb{Z}_m^* \checkmark$
• Associativity: \((ab)c = abc = a(bc) \in \mathbb{Z}_m^*\)
• Neutral element \(1 \in \mathbb{Z}_m^*\): \(1 \cdot a = a \cdot 1 = a\), for all \(a \in \mathbb{Z}_m^*\).
• Inverse element \(a^{-1}\): \(\exists a^{-1} \in \mathbb{Z}_m^*, \text{ since } \gcd(a, m) = 1 \text{ for all } a \in \mathbb{Z}_m^*\).

Solution of Problem 6

a) Substitution cipher: Keys are permutations over the symbol alphabet \(\Sigma = \{x_0, \ldots, x_{l-1}\}\).
   \(\Rightarrow\) As known from combinatorics, there are \(l!\) permutations, i.e., \(l!\) possible keys.

b) Affine cipher with key \((b, a)\) and with symbols in alphabet \(\mathbb{Z}_{26}\):
   \[c_i = (a \cdot m_i + b) \mod 26\]
   \[m_i = a^{-1} \cdot (c_i - b) \mod 26\]
   For a valid decryption \(a^{-1}\) must exist. \(a^{-1}\) exists if \(\gcd(a, 26) = 1\) holds
   \(\Rightarrow a \in \mathbb{Z}_{26}^*\). 26 has only 2 dividers as 26 = 13 \cdot 2 is its prime factorization.
   \[\mathbb{Z}_{26}^* = \{a \in \mathbb{Z}_{26} \mid \gcd(a, 26) = 1\} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \subset \mathbb{Z}_{26}\]
   \(\Rightarrow |\mathbb{Z}_{26}^*| = 12\) possible keys for \(a\).
   There is no restriction on \(b \in \mathbb{Z}_{26}\), i.e., \(|\mathbb{Z}_{26}| = 26\) possible keys for \(b\).
   Altogether, we have \(|\mathbb{Z}_{26} \times \mathbb{Z}_{26}^*| = |\mathbb{Z}_{26}| \cdot |\mathbb{Z}_{26}^*| = 26 \cdot 12 = 312\) possible keys \((a, b)\).

c) Permutation cipher with block length \(L\) \(\Rightarrow L!\) permutations \(\Rightarrow L!\) possible keys.