Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Qinwei He

Exercise 7
- Proposed Solution -

Friday, June 16, 2017

Solution of Problem 1

$$\begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} x & (x+1) & 1 & 1 \\ 1 & x & (x+1) & 1 \\ 1 & 1 & x & (x+1) \\ (x+1) & 1 & 1 & x \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \in \mathbb{F}_{2^8}^4 \tag{1}$$

It is to show that:

$$(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \equiv \sum_{i=0}^{3} r_i u^i \pmod{(u^4+1)}. \tag{2}$$

We expand the multiplication on the left hand side of (2), reduce it modulo $u^4 + 1 \in \mathbb{F}_{2^8}[u]$, and use the abbreviations $(r_0, r_1, r_2, r_3)'$ according to (1).

$$\begin{aligned}
&(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \\
= \ &c_3(x+1)u^6 + c_3u^5 + c_3u^4 + c_3xu^3 + \\
&c_2(x+1)u^5 + c_2u^4 + c_2u^3 + c_2xu^2 + \\
&c_1(x+1)u^4 + c_1u^3 + c_1u^2 + c_1xu + \\
&c_0(x+1)u^3 + c_0u^2 + c_0u + c_0x \\
= \ &[c_3(x+1)]u^6 + [c_3 + c_2(x+1)]u^5 + [c_3 + c_2 + c_1(x+1)]u^4 \\
&+ [c_3x + c_2 + c_1 + c_0(x+1)]u^3 + [c_2x + c_1 + c_0]u^2 + [c_1x + c_0]u + c_0x.
\end{aligned}$$

Now, we apply the modulo operation and merge terms:

$$\begin{aligned}
&\equiv [c_3x + c_2 + c_1 + (x+1)c_0]u^3 + [c_3(x+1) + c_2x + c_1 + c_0]u^2 + \\
&\quad [c_3 + c_2(x+1) + c_1x + c_0]u + [c_3 + c_2 + c_1(x+1) + c_0x] \\
&\overset{(1)}{\equiv} r_3u^3 + r_2u^2 + r_1u + r_0 \equiv \sum_{i=0}^{3} r_i u^i \pmod{(u^4+1)}
\end{aligned}$$

Solution of Problem 2

Given: Alphabet $\mathcal{A}$, blocklength $n \in \mathbb{N}$ and $\mathcal{M} = \mathcal{A}^n = \mathcal{C}$.
$\mathcal{A}^n$ describes all possible streams of n bits.

a) An encryption is an injective function $e_K : \mathcal{M} \to \mathcal{C}$, with $K \in \mathcal{K}$.
Fix key $K \in \mathcal{K}$. As $e(\cdot, K)$ is injective, it holds:

- $\{e(M,K) \mid M \in \mathcal{M}\} \subseteq \mathcal{C}$
- $\{e(M,K) \mid M \in \mathcal{M}\} = \mathcal{M}$
- Since $\mathcal{M} = \mathcal{C} \Rightarrow e(\mathcal{M},K) = \mathcal{C}$ also surjective
- $\Rightarrow e(\mathcal{M},K)$ is a bijective function.

A permutation π is a bijective (one-to-one) function $\pi : \mathcal{X} \to \mathcal{X}$.
$\Rightarrow$ For each K, the encryption $e(\cdot,K)$ is a permutation with $\mathcal{X} = \mathcal{A}^n$.

b) With $\mathcal{A} = \{0,1\} \Rightarrow |\mathcal{A}| = |\{0,1\}| = 2$, and $n = 6$ there are $N = 2^6 = 64$ elements.
It follows that there are $64! \approx 1.2689 \cdot 10^{89}$ different block ciphers.

Solution of Problem 3

Let $\varphi : \mathbb{N} \to \mathbb{N}$ the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$ with $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$.

a) Let $n = p$ be prime. It follows for the multiplicative group that:

$$\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p \mid \gcd(a,p) = 1\} = \{1,2,\ldots,p-1\} \Rightarrow \varphi(p) = p-1\,.$$

b) The power p^k has only one prime factor. So p^k has a common divisors that are not equal to one: These are only the multiples of p. For $1 \le a \le p^k$:

$$1 \cdot p\,, \quad 2 \cdot p\,, \quad \ldots\,, \quad p^{k-1} \cdot p = p^k\,.$$

And it follows that

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)\,.$$

c) Let $n = p\,q$ for two primes $p \neq q$. It holds for $1 \le a < p\,q$

1) $p \mid a \vee q \mid a \Rightarrow \gcd(a, p\,q) > 1$, and
2) $p \nmid a \wedge q \nmid a \Rightarrow \gcd(a, p\,q) = 1$.

It follows $\mathbb{Z}_{p\,q}^* = \underbrace{\{1 \le a \le p\,q-1\}}_{p\,q-1 \text{ elements}} \setminus \left[\underbrace{\{1 \le a \le p\,q-1 \mid p \mid a\}}_{q-1 \text{ elements}} \,\dot\cup\, \underbrace{\{1 \le a \le p\,q-1 \mid q \mid a\}}_{p-1 \text{ elements}}\right]$.
Hence: $\varphi(p\,q) = (p\,q-1)-(q-1)-(p-1) = p\,q-p-q+1 = (p-1)(q-1) = \varphi(p)\,\varphi(q)$.

d) Apply the Euler phi-function on n with the following steps:

1. Factorize all prime factors of the given n
2. Apply the rules in a) to c), correspondingly.

$\varphi(4913) = \varphi(17^3) \overset{(b)}{=} 17^2(17-1) = 4624$, and
$\varphi(899) = \varphi(30^2 - 1^2) = \varphi((30-1)(30+1)) = \varphi(29 \cdot 31) \overset{(c)}{=} 28 \cdot 30 = 840$.