Exercise 7 in Cryptography
- Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo
2015-06-18

Solution of Problem 20

a) The bit error occurs in block C_i, $i > 0$, with blocksize BS.

mode	M_i	max #err	remark
ECB	$E_K^{-1}(C_i)$	BS	only block C_i is affected
CBC	$E_K^{-1}(C_i) \oplus C_{i-1}$	BS+1	C_i and one bit in C_{i+1}
OFB	$C_i \oplus Z_i$	1	one bit in C_i, as $Z_0 = C_0, Z_i = E_K(Z_{i-1})$
CFB	$C_i \oplus E_k(C_{i-1})$	BS+1	C_i and one bit in C_{i+1}
CTR	$C_i \oplus E_K(Z_i)$	1	one bit in C_i, $Z_0 = C_0, Z_i = Z_{i-1} + 1$

b) If one bit of the ciphertext is lost or an additional one is inserted in block C_i at position j, all bits beginning with the following positions may be corrupt:

mode	block	position
ECB	i	1
CBC	i	1
OFB	i	j
CFB	i	j
CTR	i	j

In ECB and CBC, all bits of blocks C_i, C_{i+1} may be corrupt.
In OFB, CFB, CTR, all bits beginning at position j of block C_i may be corrupt.

Solution of Problem 21

Let $n \in \mathbb{N}$, $a \in \mathbb{Z}_n^*$ with $\mathbb{Z}_n^* = \{b \in \mathbb{Z}_n \mid \gcd(b, n) = 1\}$.
Consider the map $\Psi : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ defined by $\Psi(x) = ax \mod n$, with $x \in \mathbb{Z}_n^*$.

1) Show that Ψ is well-defined, i.e., $\forall x \in \mathbb{Z}_n^* \;\Rightarrow ax \in \mathbb{Z}_n^*$.
$\mathbb{Z}_n^*$ is a multiplicative group, i.e., $\forall x \in \mathbb{Z}_n^*, \forall a \in \mathbb{Z}_n^* \Rightarrow (ax) \in \mathbb{Z}_n^*$. $\square$

2) Show that Ψ is surjective, i.e., $\forall y \in \mathbb{Z}_n^* \; \exists x \in \mathbb{Z}_n^* : \Psi(x) = y$.
$y \equiv ax \pmod n \Rightarrow a^{-1}y \equiv x \pmod n \Rightarrow \Psi(a^{-1}y) \equiv y \pmod n$.
Since $\gcd(a, n) = 1$ holds for all $a \Rightarrow \exists a^{-1} \pmod n$. $\square$

3) Show that $\Psi(x)$ is injective, i.e., for $x \not\equiv y \Rightarrow \Psi(x) \not\equiv \Psi(y)$.
Indirect proof:
Let $ax \equiv ay \pmod{n}$. Since $\gcd(a,n) = 1 \Rightarrow \exists a^{-1} \in \mathbb{Z}_n^* : x \equiv y \pmod{n}$. $\square$

4) From 2) and 3) $\Rightarrow \Psi(x)$ is bijective. $\square$

5) Show that the inverse $a^{-1} \pmod{n}$ is unique.
Indirect proof:
Let $u \not\equiv v \in \mathbb{Z}_n^*$ be inverses of a, i.e., $ua \equiv 1 \pmod{n}$ and $va \equiv 1 \pmod{n}$ holds.
But $u \equiv u(va) \equiv (ua)v \equiv v \pmod{n}$ is a contradiction $\Rightarrow$ the inverse is unique.
$\Rightarrow \forall a \in \mathbb{Z}_n^*\ \exists! a^{-1}$. $\square$

6) Show that $a^{\varphi(n)} \equiv 1 \pmod{n}$:

$$1 \equiv \underbrace{(\textstyle\prod_{x\in\mathbb{Z}_n^*} x)(\prod_{x\in\mathbb{Z}_n^*} x^{-1})}_{\text{5) pairs of unique inverses}} \equiv \underbrace{(\textstyle\prod_{x\in\mathbb{Z}_n^*} \Psi(x))}_{\text{4) bijective fct.}}(\textstyle\prod_{x\in\mathbb{Z}_n^*} x^{-1}) \equiv (\prod_{x\in\mathbb{Z}_n^*} ax)(\prod_{x\in\mathbb{Z}_n^*} x^{-1})$$
$$\equiv a^{\varphi(n)}(\textstyle\prod_{x\in\mathbb{Z}_n^*} x)(\prod_{x\in\mathbb{Z}_n^*} x^{-1}) \equiv a^{\varphi(n)} \pmod{n}. \quad \blacksquare$$

Solution of Problem 22

a) By the Miller-Rabin Primality Test it will be proven that 341 is composite.
Write $n = 341 = 1 + 85 \cdot 2^2 = 1 + q \cdot 2^k$.

Algorithm 1 Miller-Rabin Primality Test (MRPT)

Write $n = 1 + q2^k, q$ odd
Choose $a \in \{2, \ldots, n-1\}$ uniformly distributed at random
$y \leftarrow a^q \mod n$
if $(y = 1)$ OR $(y = n-1)$ **then**
  return "n prime"
end if
for $(i \leftarrow 1;\ i < k;\ i{+}{+})$ **do**
  $y \leftarrow y^2 \mod n$
  if $(y = n-1)$ **then**
    return "n prime"
  end if
end for
return "n composite"

Choose $a = 2$.
Calculate $a^q \mod n$, i.e., $2^{85} \mod 341$.
Note that $2^{10} = 1024 = 3 \cdot 341 + 1 \equiv 1 \mod 341$.
It follows $2^{85} = (\underbrace{2^{10}}_{\equiv 1})^8 \cdot \underbrace{2^5}_{=32} \equiv 32 \mod 341$.
Alternatively, $2^{85} \mod 341$ is calculated by Square and Multiply, see below. As $y = 32 \notin \{1, n-1\}$ the for-loop starts with $i = 1$.
$y^2 = 32^2 = (2^5)^2 = 2^{10} \equiv 1 \mod 341$, see above.

Furthermore, $y = 1 \neq 340 \mod 341$.
As $i = 2 = k = 2$ the for-loop terminates and n is stated as composite, which is a reliable result.

b) A number n is decomposed according to MRPT as $n = 1 + q\,2^k$. It follows that MRPT has at most k squarings. The worst case occurs, if $q = 1$, then $n = 1 + 2^k \Leftrightarrow k = \log_2(n-1)$. With n having 300 digits it follows: $n < 10^{301} = (\underbrace{10^3}_{<2^{10}})^{100} \cdot \underbrace{10}_{<2^4} < 2^{1004} \Rightarrow$

$k \leq 1004$.
Consequently, less than 1004 squarings are needed. ($k \approx 999.9$)

Note, evaluating $a^q \mod n$ with Square and Multiply takes t squarings. But as $2^t \leq q$ holds, the worst case is reached, for equality which means $t = 0$, i.e., $q = 1$, as otherwise q would be not odd.

Determining $2^{85} \mod 341$ by Square and Multiply.
It holds $a = 2$, $x = 85 = (1010101)_2$, i.e., $t = 6$.

Algorithm 2 Square and multiply

Require: $x = (x_t, \ldots, x_0) \in \mathbb{N}, a \in \mathbb{N}$
Ensure: $a^x \mod n$

```
y ← a
for (i = t − 1, i ≥ 0, i--) do
    y ← y^2 mod n
    if (x_i = 1) then
        y ← y · a mod n
    end if
end for
return y
```

The following tabular denotes the evaluation of the Square and Multiply algorithm. The table is initialized in the first line with $i = t = 6$ and $y = 1$. There are $t + 1$ lines numbered from t down to 0. The binary representation of $x = (x_t. \ldots .x_0)$ is given in column two. Using those values the columns four and five are evaluated row by row. For each row the y value is taken from the last column of the row above. The final value in the fifth column is the result of $a^x \mod n$.

i	x_i	y	$y^2 \mod n$	$y^2(1 + x_i \cdot (a-1)) \mod n$
6	1	1	1	2
5	0	2	4	4
4	1	4	16	32
3	0	32	$1024 \equiv 1 \mod 341$	1
2	1	1	1	2
1	0	2	4	4
0	1	4	16	32

The solution is $2^{85} \equiv 32 \mod 341$.

Solution of Problem 23

Chinese Remainder Theorem:
Let $m_1, \ldots, m_r$ be pair-wise relatively prime, i.e., $\gcd(m_i, m_j) = 1$ for all $i \neq j \in \{1, \ldots, r\}$, and furthermore let $a_1, \ldots, a_r \in \mathbb{N}$. Then, the system of congruences

$$x \equiv a_i \pmod{m_i},\ i = 1, \ldots, r,$$

has a unique solution modulo $M = \prod_{i=1}^{r} m_i$ given by

$$x \equiv \sum_{i=1}^{r} a_i M_i y_i \pmod{M}, \tag{1}$$

where $M_i = \frac{M}{m_i}$, $y_i = M_i^{-1} \pmod{m_i}$, for $i = 1, \ldots, r$.

a) Show that (1) is a valid solution for the system of congruences:
Let $i \neq j \in \{1, \ldots, r\}$. Since $m_j \mid M_i$ holds for all $i \neq j$, it follows:

$$M_i \equiv 0 \pmod{m_j}. \tag{2}$$

Furthermore, we have $y_j M_j \equiv 1 \pmod{m_j}$.
Note that from coprime factors of M, we obtain:

$$\gcd(M_j, m_j) = 1 \Rightarrow \exists\, y_j \equiv M_j^{-1} \pmod{m_j}, \tag{3}$$

and the solution of (1) modulo a corresponding m_j can be simplified to:

$$x \equiv \sum_{i=1}^{r} a_i M_i y_i \overset{(2)}{\equiv} a_j M_j y_j \overset{(3)}{\equiv} a_j \pmod{m_j}.$$

b) Show that the given solution is unique for the system of congruences:
Assume that two different solutions y, z exist:

$$\begin{aligned}
y \equiv a_i \pmod{m_i}\ &\wedge\ z \equiv a_i \pmod{m_i},\ i = 1, \ldots, r,\\
\Rightarrow 0 &\equiv (y - z) \pmod{m_i}\\
\Rightarrow m_i &\mid (y - z)\\
\Rightarrow M &\mid (y - z), \text{ as } m_1, \ldots, m_r \text{ are relatively prime for } i = 1, \ldots, r,\\
\Rightarrow y &\equiv z \pmod{M}.
\end{aligned}$$

This is a contradiction, therefore the solution is unique.