T-79.503 [old: T-110.503] Foundations of Cryptology
Exam
December 15, 2003

SOLUTIONS

1. a) The unicity distance n_0 can be estimated using the formula

$$n_0 \approx \frac{\log_2 |\mathcal{K}|}{R \log_2 |\mathcal{P}|} = \frac{\log_2 |2^m|}{R \log_2 2} = \frac{m}{R}$$

since the key is randomly generated string of m bits, and the plaintext is one bit.

b) From the given information about the plaintext redundancy we get, for each third plaintext bit the following equations:

$$\begin{cases} x_3 &= x_1 + x_2 = k_1 + k_2 + 1 \\ x_3 &= k_3 \end{cases}$$
$$\begin{cases} x_6 &= x_4 + x_5 = k_4 + k_5 + 1 \\ x_6 &= k_1 + 1 \end{cases}$$
$$\begin{cases} x_9 &= x_7 + x_8 = k_2 + k_3 \\ x_9 &= k_4 + 1 \end{cases}$$
$$\begin{cases} x_{12} &= x_{10} + x_{11} = k_5 + k_1 + 1 \\ x_{12} &= k_2 \end{cases}$$
$$\begin{cases} x_{15} &= x_{13} + x_{14} = k_3 + k_4 \\ x_{15} &= k_5 + 1 \end{cases}$$

The resulting system of five equations and five unknown key bits

$$\begin{array}{ccccccccccc} k_1 & + & k_2 & + & k_3 & & & & & = & 1 \\ k_1 & & & & & + & k_4 & + & k_5 & = & 0 \\ & & k_2 & + & k_3 & + & k_4 & & & = & 1 \\ k_1 & + & k_2 & & & & & + & k_5 & = & 1 \\ & & & & k_3 & + & k_4 & + & k_5 & = & 1 \end{array}$$

is easy to solve since in suitably chosen sets of three equations one unknown appears only once, while the other four unknowns appear twice each. By summing up the first three equations gives $k_5 = 0$, by summing up equations 1, 2 and 5, gives $k_2 = 0$. Equations 2, 3 and 4 give $k_3 = 0$, equations 3, 4 and 5 give $k_1 = 1$ and equations 1, 4 and 5 give $k_4 = 1$. Hence the key is $K = (1, 0, 0, 1, 0)$.

2. From the given plaintext and ciphertext we get two equations for R_1

$$\begin{cases} R_1 &= 100 + f(001 + K) \text{ (encryting over the first round)} \\ R_1 = L_2 &= 100 + f(110 + K^3) \text{ (decrypting over the third round)} \end{cases}$$

It follows that

$$f(001 + K) = f(110 + K^3). \qquad (1)$$

Since f is a bijection in $\mathbb{F} = \mathbb{Z}_2[x]/(x^3+x+1)$ it follows that (1) can hold if and only if

$$001 + K = 110 + K^3$$

which is equivalent to

$$K + K^3 = 111 \tag{2}$$

To find a solution $K \in \mathbb{F}$, we compute the values of $z + z^3$ for all $z \in \mathbb{F}$:

z	z^3	$z+z^3$
000	000	000
001	001	000
010	011	001
011	100	111
100	101	001
101	110	011
111	010	101

It follows that there is a unique solution $K = 011$ that satisfies equation (2).

3. First the inverse of 15 modulo 2003 is computed using the Euclidean algorithm. It is 1736, and by multiplying the first equation the system is transformed to:

$$\begin{aligned} x &= 802 \pmod{2003} \\ x &= 12 \pmod{2004} \end{aligned}$$

We denote $m_1 = 2003$ and $m_2 = 2004$. Then $\gcd(m_1, m_2)$=1 and we can apply the Chinese Remainder Theorem. We get $M_1 = 2004$, $M_2 = 2003$, $y_1 = M_1^{-1} \bmod m_1 = 1$, $y_2 = M_2^{-1} \bmod m_2 = -1 = 2003$, from where we get

$$x = 802 \cdot 2004 \cdot 1 + 12 \cdot 2003 \cdot 2003 = 1583172 \,(\mathrm{mod} 4014012).$$

4. If the Pollard $p-1$ algorithm works then a nontrivial divisor of 15122003 can be found as the gcd of 1655213 -1 and 15122003. Using the Euclidean algorithm we get gcd(1655212,15122003) = 13, and obtain the factorisation

$$15122003 = 13 \cdot 1163231.$$

Pollard's algorithm works because $p - 1 = 12 \,|\, 4!$.

5. Given a message $x \in \mathbb{Z}_{30}$ the El Gamal signature of x is (δ, γ) where

$$\begin{aligned} \gamma &= 3^k \bmod 31 \\ \delta &= (x - a\gamma)k^{-1} \bmod 30. \end{aligned}$$

Given two signatures we get the following information

$$\begin{aligned} 24 &= 3^k \bmod 31 && (3) \\ 7 &= (25 - 24a)k^{-1} \bmod 30 && (4) \\ 17 &= (5 - 24a)k^{-1} \bmod 30. && (5) \end{aligned}$$

We can try to solve a from (4) and (5) by eliminating the unknown k first. For this purpose we multiply (4) with $17k$ to get:

$$29k \equiv 5 + 12a (\mathrm{mod} 30)$$

and (5) with $7k$ and get

$$29k \equiv 5 + 12a (\mathrm{mod} 30).$$

Unfortunately, the resulting equations are the same. If k is eliminated, everything is eliminated. Therefore we cannot derive any explicit information of a. But, as somebody noticed, the given two signatures can be used to generate new valid signatures for all messages x that can be expressed as $tx_1 - (t-1)x_2$. For example, $15 = (2 \cdot 25 - 5) \bmod 30$, and a valid signature for $x = 15$ can be created as $(24, \delta)$ with $\delta = 2\delta_1 - \delta_2 = 27$. Verify!

A second approach to this problem is to try to solve for k first. By eliminating a from (4) and (5) one gets $20k \equiv 20 \bmod 30$. Dividing this conruence with 10 we obtain $k \equiv 1 \bmod 3$. Since k is invertible modulo 30, the possible values for k are: 1, 7, 13, and 19. We compute 3^k for this candidates, and get $3^1 = 3$, $3^7 \bmod 31 = 17$, $3^{13} \bmod 31 = 24$, and finally, $3^{19} \bmod 31 = 12$. We compare the obtained values with the known value of $\gamma = 24$. So we found a unique value for k, that is $k = 13$. By substituting it to (3) or (4) gives $6a \equiv 6 \pmod{30}$. Dividing this congruence with 6, gives $a \equiv 1 \pmod{5}$.