TIK-110.503 Foundations of Cryptology
Final exam
16.12.1999

1. The bit length of DES key is 56 bits and DES block is 64 bits.

   a) There are $|\mathcal{P}| = 4$ possible plaintext blocks of four bits. Hence the redundancy of the plaintext is $R_L = 1 - \frac{\log_2 |\mathcal{P}|}{\log_2 2^4} = 1 - \frac{2}{4} = \frac{1}{2}$. Hence the unicity distance is $n_0 = \frac{\log_2 2^{56}}{R_L \log_2 2^{64}} = 1.75$ DES blocks $= 112$ bits.

   b) Now there are $|\mathcal{P}| = 4 \cdot 16 = 2^6$ possible plaintext blocks of eight bits. Hence the redundancy of the plaintext is $R_L = 1 - \frac{\log_2 |\mathcal{P}|}{\log_2 2^8} = 1 - \frac{6}{8} = \frac{1}{4}$. Hence the unicity distance is $n_0 = \frac{\log_2 2^{56}}{R_L \log_2 2^{64}} = 3.5$ DES blocks $= 224$ bits.

2. Observe that if, for all $i = 1, \ldots, r$, there is a round key K_i' such that

$$F_i(c(R_{i-1}) \oplus K_i') = F_i(R_{i-1} \oplus K_i) \tag{1}$$

   then we have

$$\begin{aligned} c(L_i) &= c(R_{i-1}) \\ c(R_i) &= c(L_{i-1}) \oplus F_i(c(R_{i-1}) \oplus K_i'), \end{aligned}$$

   for all i, and consequently the plaintext c(X) is encrypted to c(Y). Clearly, $K_i' = c(K_i)$ satisfies condition (1). (See also Stinson, Exercise 3.2.)

3. Recall that 1999 is prime. Note also that $1999 \equiv 3 (\mathrm{mod} 4)$.

   a) 12 is a quadratic non-residue modulo 1999 if and only if the Legendre symbol $\left(\frac{12}{1999}\right)$ is equal to -1. We compute the Legendre (Jacobi) symbol:

$$\left(\frac{12}{1999}\right) = \left(\frac{2}{1999}\right)^2 \left(\frac{3}{1999}\right) = \left(\frac{3}{1999}\right) = -\left(\frac{1999}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

   b) Writing the congruence $16^x \equiv 12 (\mathrm{mod} 1999)$ in the form $(4^x)^2 \equiv 12 (\mathrm{mod} 1999)$ we see that it has solutions only if 12 is a quadratic residue modulo 1999. Hence, by a), the congruence does not have solutions.

4. First, using the Chinese Remainder Theorem, we find y, $0 < y < n_1 \cdot n_2$ such that $y \equiv y_i$ (mod n_i). For this purpose, we need to compute the inverses of the moduli with respect to each other. Denote $u = 2183^{-1} \bmod 2173 = 10^{-1} \bmod 2173$. Then $10 \cdot u = 1 + 2173 \cdot k$, for some integer k. Clearly $k = 3$ works, because $3 \cdot 3 = 9 = -1 (\mathrm{mod} 10)$, and we get $u = 652$. Similarily, denote $v = 2173^{-1} \bmod 2183 = (-10)^{-1} \bmod 2183$. Then $10 \cdot v = -1 + 2183 \cdot k$, for some suitable k. Now $k = 7$ works, because $3 \cdot 7 = 1 (\mathrm{mod} 10)$, and we get $v = (2183 \cdot 7 - 1)/10 = 1528$. Using CRT, we get $y = 2027 \cdot 652 \cdot 2183 + 1111 \cdot 2173 \cdot 1528 \bmod 4743659 = 3996001 = (1999)^2$. We get $x = 1999$.

5. Element $\alpha = x$ is primitive and generates the entire $GF(2^4)^*$ with polynomial $x^4 + x + 1$:

$$\begin{aligned} \alpha^0 &= 1 \\ \alpha^1 &= x \\ \alpha^2 &= x^2 \\ \alpha^3 &= x^3 \\ \alpha^4 &= x + 1 \\ \alpha^5 &= x^2 + x \end{aligned}$$

$$
\begin{aligned}
\alpha^6 &= x^3 + x^2 \\
\alpha^7 &= x^3 + x + 1 \\
\alpha^8 &= x^2 + 1 \\
\alpha^9 &= x^3 + x \\
\alpha^{10} &= x^2 + x + 1 \\
\alpha^{11} &= x^3 + x^2 + 1 \\
\alpha^{12} &= x^3 + x^2 + x + 1 \\
\alpha^{13} &= x^3 + x^2 + 1 \\
\alpha^{14} &= x^3 + 1 \\
\alpha^{15} &= 1
\end{aligned}
$$

The order of the entire multiplicative group is 15. Hence it has strict subgroups of orders 1, 3 and 5, which we denote by S_1, S_3 and S_5, respectively. The generators of these groups are 1, $\alpha^{15/3} = \alpha^5$ and $\alpha^{15/5} = \alpha^3$ (also respectively). We obtain:

$$
\begin{aligned}
S_1 &= \{1\} \\
S_3 &= \{1, x^2 + x, x^2 + x + 1\} \\
S_5 &= \{1, x^3, x^3 + x^2, x^3 + x, x^3 + x^2 + x + 1\}.
\end{aligned}
$$