Mid Semester Examination, Autumn 2003-04

Solutions

---

1. Let $m = m_0 m_1 \ldots m_{l-1}$ be the plaintext and $c = c_0 c_1 \ldots c_{l-1}$ the corresponding ciphertext. We have $l := |m| = |c| = 54$. Since Y has code 24 and H has code 7 and $m_0 =$ H, it follows that $t = 24 - 7 = 17$. So we can translate back the ciphertext to get the intermediate string $x = x_0 x_1 \ldots x_{l-1}$ with $x_i = m_{si \,\mathrm{rem}\, 54}$:

$x =$ H␣GO␣EBITELOEYLLMS␣EOB␣TV␣␣IUECTNENAO␣S␣R␣SDPRVCAMYEOY

Now we have to apply the reverse permutation to get back m. It easily follows that $m_i = x_{s^{-1} i \,\mathrm{rem}\, 54}$, where $ss^{-1} \equiv 1 \pmod{54}$. The following table lists the decrypted message for all the possibilities of s with $\gcd(s, l) = 1$.

s	s^{-1}	Recovered plaintext
1	1	H␣GO␣EBITELOEYLLMS␣EOB␣TV␣␣IUECTNENAO␣S␣R␣SDPRVCAMYEOY
5	11	HO␣EP␣ETNRGYVAVOL␣OC␣L␣␣AEMISMBSU␣YI␣ERETEC␣OEOTSYLBND
7	31	HTT␣MCV␣NERSA␣GEL␣␣M␣ONOSEYI␣AEDOEUEOYPBOEB␣LR␣YCISLVT
11	5	HELLO␣CARRY␣BOMB␣TO␣VEGIES␣IN␣SCOOTY␣TUESDAY␣ELEVEN␣PM
13	25	H␣YBVSSYSENEC␣␣E␣C␣DL␣LABTGIOTAEPLROOINOUYVMORM␣E␣TE␣E
17	35	HAMENYAELR␣IST␣␣O␣OSOELMCOVITDVERBG␣␣YNLYTECUEP␣B␣␣OSE
19	37	H␣OORTBD␣EVEEMNLOA␣␣SB␣␣VIPILCCYYEMYOEG␣␣ES␣TRUOATLENS
23	47	HCRE␣EEEORSTVSLOYDOE␣LT␣A␣NIOYBYV␣N␣␣O␣EP␣CTMEGMSAUBLI
25	13	HY␣␣OOV␣YE␣AAIOEVE␣TPOMES␣LIRYE␣SELTOMTBNCBENR␣SCDGLU␣
29	41	H␣ULGDCS␣RNEBCNBTMOTLES␣EYRIL␣SEMOPT␣EVEOIAA␣EY␣VOO␣␣Y
31	7	HILBUASMGEMTC␣PE␣O␣␣N␣VYBYOIN␣A␣TL␣EODYOLSVTSROEEE␣ERC
35	17	HSNELTAOURT␣SE␣␣GEOYMEYYCCLIPIV␣␣BS␣␣AOLNMEEVE␣DBTROO␣
37	19	HESO␣␣B␣PEUCETYLNY␣␣GBREVDTIVOCMLEOSO␣O␣␣TSI␣RLEAYNEMA
41	29	HE␣ET␣E␣MROMVYUONIOORLPEATOIGTBAL␣LD␣C␣E␣␣CENESYSSVBY␣
43	49	HMP␣NEVELE␣YADSEUT␣YTOOCS␣NI␣SEIGEV␣OT␣BMOB␣YRRAC␣OLLE
47	23	HTVLSICY␣RL␣BEOBPYOEUEODEA␣IYESONO␣M␣␣LEG␣ASREN␣VCM␣TT
49	43	HDNBLYSTOEO␣CETERE␣IY␣USBMSIMEA␣␣L␣CO␣LOVAVYGRNTE␣PE␣O
53	53	HYOEYMACVRPDS␣R␣S␣OANENTCEUI␣␣VT␣BOE␣SMLLYEOLETIBE␣OG␣

In practice one need not compute this complete table. Looking at the recovered letter m_1 we can throw away most of the possibilities, namely, all but $s = 11, 37, 41$. Finally, recovering m_2 for these three values lets us uniquely identify s as $s = 11$. The corresponding plaintext is:

$m =$ HELLO␣CARRY␣BOMB␣TO␣VEGIES␣IN␣SCOOTY␣TUESDAY␣ELEVEN␣PM

2. DES key schedule permutes the 56 bits of the key and performs cyclic shifts on its two halves. Both permuting and shifting commute with complementing and so the key schedule of $\overline{K}$ gives the round keys $\overline{K_1}, \overline{K_2}, \ldots, \overline{K_{16}}$, where $K_1, K_2, \ldots, K_{16}$ are the round keys for K. In an awful notation this translates to $\overline{K}_i = \overline{K_i}$ for $i = 1, \ldots, 16$.

Now look at the f function of DES. For inputs A and J of f we have $f(A, J) = P(S(E(A) \oplus J))$. Complementing both A and J yields $E(\overline{A}) \oplus \overline{J} = \overline{E(A)} \oplus \overline{J} = (1^{48} \oplus E(A)) \oplus (1^{48} \oplus J) = E(A) \oplus J$, i.e., $f(\overline{A}, \overline{J}) = f(A, J)$. Here 1^l denote the bit-string of length l consisting of all 1 bits.

Finally, investigate the DES encryption rounds. If I complement x, the values L_0 and R_0 get complemented (since any permutation and, in particular, IP commutes with complementation). Denoting the L_i and R_i values for $\overline{x}$ by L'_i and R'_i (and those for x by simply L_i and R_i) we see that $L'_0 = \overline{L_0}$ and $R'_0 = \overline{R_0}$. If $L'_{i-1} = \overline{L_{i-1}}$ and $R'_{i-1} = \overline{R_{i-1}}$ for some $i = 1, \ldots, 16$, we have $L'_i = R'_{i-1} = \overline{R_{i-1}} = \overline{L_i}$. Also $R'_i = L'_{i-1} \oplus f(R'_{i-1}, \overline{K}_i) = \overline{L_{i-1}} \oplus f(\overline{R_{i-1}}, \overline{K_i}) = \overline{L_{i-1}} \oplus f(R_{i-1}, K_i) = 1^{32} \oplus L_{i-1} \oplus f(R_{i-1}, K_i) = 1^{32} \oplus R_i = \overline{R_i}$. Repeating this argument for $i = 1, \ldots, 16$ gives $L'_{16} = \overline{L_{16}}$ and $R'_{16} = \overline{R_{16}}$ and so $\mathrm{DES}_{\overline{K}}(\bar{x}) = \mathrm{IP}^{-1}(R'_{16} \,||\, L'_{16}) = \mathrm{IP}^{-1}(\overline{R_{16}} \,||\, \overline{L_{16}}) = \overline{\mathrm{IP}^{-1}(R_{16} \,||\, L_{16})} = \overline{\mathrm{DES}_K(x)}$.

3. (a) Initializing any LFSR of length n to the state α gives an output bit-stream whose leftmost n bits are $a_0, a_1, \ldots, a_{n-1}$. Thus $L(\alpha) \leqslant n$.

[if] Let $\alpha = 00\ldots01$. By Part (a) $L(\alpha) \leqslant n$. Suppose that $L(\alpha) < n$, i.e., some LFSR R of length $l < n$ generates α as the first n bits. This requires R to have the initial state $a_0a_1\ldots a_{l-1} = 00\ldots0$, and so R will output only 0 bits, a contradiction to the fact that $a_{n-1} = 1$. Thus $L(\alpha) = n$.

[only if] Suppose that $\alpha \neq 00\ldots01$. Also α is non-zero. So $a_j = 1$ for some $j \in \{0, 1, \ldots, n-2\}$. Let R be an LFSR of length $n-1$, with control connections $c_1, \ldots, c_{n-1}$ and initialized to the state $a_0a_1\ldots a_{n-2}$. If $a_{n-1} = 0$, then taking $c_1 = c_2 = \cdots = c_{n-1} = 0$ will allow R to output a bit-string with α as the leftmost part. If $a_{n-1} = 1$, then taking $c_i = \begin{cases} 1 & \text{if } i = n-j-1 \\ 0 & \text{otherwise} \end{cases}$ will let R generate a bit-string with α as the leftmost part. Thus $L(\alpha) \leqslant n-1$.

4. I will prove the contrapositive, that is, if it is easy to find collisions for H', then it is also easy to find collisions for H. Let $(x_1, x_2) \in \{0,1\}^{4m} \times \{0,1\}^{4m}$ be a collision for H', i.e., $x_1 \neq x_2$, but $H'(x_1) = H'(x_2)$. Break up x_1 and x_2 as $x_1 = L_1 \,||\, R_1$ and $x_2 = L_2 \,||\, R_2$. If $L_1 \neq L_2$, but $H(L_1) = H(L_2)$, then (L_1, L_2) is a collision for H. Similarly, if $R_1 \neq R_2$, but $H(R_1) = H(R_2)$, then (R_1, R_2) is a collision for H. So assume that either $H(L_1) \neq H(L_2)$ or $H(R_1) \neq H(R_2)$. But then $y_1 := H(L_1) \,||\, H(R_1)$ and $y_2 := H(L_2) \,||\, H(R_2)$ are distinct, whereas $H(y_1) = H(y_2)$, i.e., (y_1, y_2) is a collision for H.

5. **(a)** $\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{1\cdot2\cdots k}$ is an integer. The denominator in this expression for $\binom{p}{k}$ is not divisible by p for $k \in \{1, 2, \ldots, p-1\}$, whereas the numerator is.

(b) Applying induction on n makes it sufficient to solve the exercise only for $n = 1$. By the binomial theorem $(a+b)^p = a^p + \left(\sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k\right) + b^p$. Now use Part (a).

(c) By Part (b) we have $f(X)^2 = a_0^2 + a_1^2X^2 + a_2^2X^4 + \cdots + a_d^2X^{2d}$. Since $a^2 = a$ for each $a \in \mathbb{Z}_2$, it follows that $f(X)^2 = a_0 + a_1X^2 + a_2X^4 + \cdots + a_dX^{2d}$ in $\mathbb{Z}_2[X]$.

6. The set G of all bijective functions $\mathbb{Z} \to \mathbb{Z}$ is a group under functional composition. The identity in this group is the identity map $\mathrm{id}_{\mathbb{Z}}$. Take:

$$g(n) := \begin{cases} n+1 & \text{if } n \text{ is odd,} \\ n-1 & \text{if } n \text{ is even,} \end{cases}$$
$$h(n) := \begin{cases} n+1 & \text{if } n \text{ is even,} \\ n-1 & \text{if } n \text{ is odd.} \end{cases}$$

It is clear that $g \circ g = \mathrm{id}_{\mathbb{Z}} = h \circ h$, i.e., both g and h are of order 2. Denote $f := g \circ h$. We have:

$$f(n) = \begin{cases} n+2 & \text{if } n \text{ is even,} \\ n-2 & \text{if } n \text{ is odd.} \end{cases}$$

But then for any $k \in \mathbb{N}$ the k-fold composition f^k of f is given by:

$$f^k(n) = \begin{cases} n+2k & \text{if } n \text{ is even,} \\ n-2k & \text{if } n \text{ is odd.} \end{cases}$$

It follows that the functions $f^1, f^2, f^3, \ldots$ are all distinct (and neither is the identity map). Therefore, f is of infinite order.

(Note that you can perhaps locate such beasts among matrices, i.e., in the special linear group (over $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$). I require a *proof* that your product matrix is of infinite order.)