Mid Semester Examination, Autumn 2003-04

Total points: 50 | September 20, 2003 | Total time: $2 + \epsilon$ hours

---

1. Suppose that some terrorists of Foeland are trying to mount an attack somewhere in our institute and our intelligence agencies intercepted the following message (`YQXEQVSZJ...COVEO`) of Foe terrorists. I have added the indices of the letters in the intercepted string for your convenience.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Y	Q	X	E	Q	V	S	Z	J	V	B	E	V	O	B	B	C	I	Q	V	E	S	Q	J	L	Q	Q

27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
Z	K	V	T	J	D	V	D	R	E	Q	I	Q	H	Q	I	U	F	H	L	T	R	C	O	V	E	O

Suppose also that the encryption algorithm of Foes is as follows: Foes use the alphabet $\{\texttt{A}, \texttt{B}, \texttt{C}, \ldots, \texttt{Z}, \texttt{␣}\}$ for plaintext and ciphertext messages, where ␣ denotes space, and they know no language other than English. They give the code 0 to `A`, 1 to `B`, ..., 25 to `Z` and 26 to space. They use a pair (s, t) of integers as the key. Given a plaintext message m of l letters with $\gcd(s, l) = 1$, they pick up every s-th letter from m in a wrap-around fashion (starting from the leftmost letter), until all the letters in the plaintext string are exhausted. Then they translate (the code of) each letter in the resulting sequence by t modulo 27 and use the translated string as the ciphertext message c. Mathematically, if $m = m_0 m_1 \ldots m_{l-1}$ is the plaintext, then the ciphertext $c = c_0 c_1 \ldots c_{l-1}$ is given by $c_i = (m_{si \bmod l} + t) \bmod 27$. For example, if the plaintext is `ABC␣XYZ` and $(s, t) = (2, 3)$, then picking up every second letter gives `ACXZB␣Y` and translation of each letter by three positions gives `DF␣BECA`.

It is known that every plaintext message among Foes starts with `HELLO`. Use this information to deduce the secret key (s, t) for the message of terrorists, mentioned above. Also recover the plaintext message. **(6+6)**

2. For a bit-string s let $\overline{s}$ denote the bit-wise complement of s. Deduce that $\mathrm{DES}_{\overline{K}}(\overline{x}) = \overline{\mathrm{DES}_K(x)}$, that is, complementing both the plaintext message and the key complements the ciphertext message. **(9)**

3. Let $\alpha = a_0 a_1 \ldots a_{n-1} \neq 00 \ldots 0$ be a bit-string of length $n \geqslant 1$. The *linear complexity* $L(\alpha)$ of α is defined to be the length of the shortest LFSR that generates α as the leftmost part of its output (when it is initialized to a suitable state). Prove that:

(a) $L(\alpha) \leqslant n$. **(3)**

(b) $L(\alpha) = n$, if and only if $\alpha = 00 \ldots 01$. **(6)**

4. Given a compression function $H : \{0,1\}^{2m} \to \{0,1\}^m$, define a compression function $H' : \{0,1\}^{4m} \to \{0,1\}^m$ as follows. Let x be a string of bit-length $4m$. Write $x = L \,||\, R$, where each of L and R is of length $2m$ bits. Define $H'(x) := H(H(L) \,||\, H(R))$. Show that if H is collision-resistant, then H' is also collision-resistant. **(8)**

5. Let p be a prime.

(a) Show that the binomial coefficient $\binom{p}{k}$ is divisible by p for all $k = 1, 2, \ldots, p-1$. **(4)**

(b) Let A be an integral domain of characteristic p (for example, $A = \mathbb{Z}_p$ or $\mathbb{Z}_p[X]$) and let $a, b \in A$. Prove that $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ for all $n = 1, 2, 3, \ldots$. **(4)**

(c) Let $f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d \in \mathbb{Z}_2[X]$ (with each $a_i \in \{0,1\}$). Demonstrate that $f(X)^2 = a_0 + a_1 X^2 + a_2 X^4 + \cdots + a_d X^{2d}$. **(4)**

6. [*Bonus exercise*] Give an example of a group $(G, \diamond)$ and of elements $g, h \in G$, such that g and h are of finite order (in G), whereas $g \diamond h$ is of infinite order. (Note that such silly incidents do not occur in groups that are finite or Abelian. In this course we will do cryptography only in finite Abelian groups. However, infinite non-Abelian groups (like Artin's braid groups) are nowadays used in cryptography. This exercise is not too crazy for this day then.) **(15)**

Dr. Abhijit Das, Dept. of Computer Science & Engg, Indian Institute of Technology, Kharagpur 721 302