

Homework Ten Solutions

Due Friday, December 6th, 2002, at 5:00pm.

Your task

A simple encryption mechanism

The Implausible One-Time Pad Company markets an encryption product that encrypts a plaintext sequence of letters and spaces using a one-word key. The algorithm used by this product is to translate the plaintext and key into numbers using the rule 0=Space, 1=A, 2=B, ..., 26=Z, and then add the first letter of the plaintext to the first letter of the key, the second letter to the second letter, and so on, repeating the key when one runs out of letters. The resulting sums are then converted to their remainders when divided by 27, and translated back into letters using the rule.

For example, here is how the plaintext EAT YOUR VEGETABLES is encrypted with the key DAILY to produce the ciphertext IBBLSV LTIHNEZFMND:

Plaintext:	E	A	T	-	Y	O	U	R	-	V	E	G	E	T	A	B	L	E	S
In numbers:	5	1	20	0	25	15	21	18	0	22	5	7	5	20	1	2	12	5	19
Key:	D	A	I	L	Y	D	A	I	L	Y	D	A	I	L	Y	D	A	I	L
In numbers:	4	1	9	12	25	4	1	9	12	25	4	1	9	12	25	4	1	9	12
Sum:	9	2	29	12	50	19	22	27	12	47	9	8	14	32	26	6	13	14	31
Remainder:	9	2	2	12	23	19	22	0	12	20	9	8	14	5	26	6	13	14	4
Ciphertext:	I	B	B	L	W	S	V	-	L	T	I	H	N	E	Z	F	M	N	D

1. Find the plaintext whose ciphertext encoded with the key HM is MN KHBIDA.
2. Show that the Implausible One-Time Pad is vulnerable to a chosen plaintext attack, i.e., that if you can get somebody to encrypt a plaintext of your choice with their key and show you the result, then you can recover any other plaintext encoded with that key.

Some artificial problems

Do problems 15 and 26 from pages 448–449 of Brookshear. For problem 26, assume that the operation of pouring water from one bucket can only be stopped when the source bucket is empty or the target bucket is full.

Submitting your solutions

Write up an email message containing your full name and the answer to these problems in plain text format (this means no HTML or Microsoft word documents), and send it to aspnes+110-02-10@cs.yale.edu. (Note: this is **not** the same email address as for previous homework.)

Solution:

A simple encryption mechanism

1. EASY PART

2. The easiest way to do this is probably to choose a plaintext consisting of all spaces. Since a space maps to zero, each letter of the ciphertext will be equal to the corresponding letter of the key. If your chosen plaintext is long enough, you should be able to guess where the key repeats.

Problem 15

Player X should select move B. If she selects B, she can obtain at least a tie no matter what Y does. But if she selects A, player Y can respond with the middle move and force X to lose. The difference between the choices a two-person game and a one-person game is that in a one-person game it is enough to find a single path to some winning state, but in a two-person game the choice of move must take into account all possible responses by the opponent, meaning that much more of the state space may need to be examined.

Problem 26

States of the system describe the amount of water in the two buckets. For example, we might write the state in which both buckets are empty as $(0,0)$ and the state in which both buckets are full as $(3,5)$. Productions are operations on states corresponding to emptying a bucket (e.g. $(x,y) \rightarrow (0,y)$), filling a bucket (e.g. $(x,y) \rightarrow (x,5)$), or filling one bucket from another (e.g. $(3,1) \rightarrow (0,4)$ or $(3,4) \rightarrow (2,5)$). For this problem the best control system may just be breadth-first search; it is not at all obvious what sort of heuristic might help to find the solution sequence $(0,0) \rightarrow (0,5) \rightarrow (3,2) \rightarrow (0,2) \rightarrow (2,0) \rightarrow (2,5) \rightarrow (3,4) \rightarrow (0,4)$.