IV054 Coding, Cryptography and Cryptographic Protocols
2013 - Exercises IV.

1. Decrypt the following cryptotexts.

   (a) `WIWGC RYC CXA VYC VYMW LGXUGWOO. WIWGC OSWL VYC QW BGAHSBAN. CWS SEWGW DHNN OSGWSPE XAS QWBXGW CXA YZ WIWG-NWZUSEWZHZU, WIWG-YOPWZRHZU, WIWG-HVLGXIHZU LYSE. CXA MZXD CXA DHNN ZWIWG UWS SX SEW WZR XB SEW FXAGZWC. QAS SEHO, OX BYG BGXV RHOPXAGYUHZU, XZNC YRRO SX SEW FXC YZR UNXGC XB SEW PNHVQ.`

   (b) `DZYOH HIBYG ITZYL IUODW TYKHS KBKOJ TZOXY DIGUM XUDID MDIKB GITZY LEZYL YIBYO GZJYD DYLIB OBOJT ZOXYD IUSOT TYPDK IDUBM SYLIG YCMIV OJYBD YBGLW TDYPM UIBQO UISTJ YSODZ YSODI GOJHM BGDIK BOBPG KBVYL DYPXO GADKO JYDDY L`

   (c) `0-13-066943-1  0-471-08132-9  0-684-83130-9  0-8476-7438-X 0-8493-8523-7  0-387-94293-9  978-1-420-07146-7`

   (d) `MAIDEN POET`

2. You have captured cryptotext encrypted with the Vigenère cipher such that the string `GIEFPHIH` starts at positions 7, 1253 and 2261. Estimate the key length.

3. Consider the Hill cryptosystem with an $n \times n$ matrix H and the English alphabet used.

   (a) Is the cryptosystem perfectly secure, if we use it to send n encrypted blocks of length n? (Assume that all possible messages are sent with the same probability.)

   (b) If not, formulate a necessary and sufficient condition for the plaintext blocks so that the cryptosystem is perfectly secure.

   (c) How many blocks that obey this condition can be sent at most using the same matrix H?

4. Construct as minimum as possible cryptosystem S and two different key distributions P_K and P'_K such that S_{P_K} and $S_{P'_K}$ are both perfectly secure.

5. Perform the known-plaintext attack against 2×2 key matrix of the Hill cryptosystem if you obtained plaintext/ciphertext couple `lesf`/`DMFX`.

6. Consider the cryptosystem which uses the table given below to encrypt letters into 1-digit or 2-digit numbers. Letters from the first row are encrypted with the digit in the corresponding column whereas a letter from the second or third row is encrypted with the digit in the corresponding row followed with the digit in the corresponding column, *eg.* S $\rightarrow$ 7, Q $\rightarrow$ 61. In the second cipher stage, modulo 10 subtraction of a secret key number is performed.

	0	1	2	3	4	5	6	7	8	9
	A	T		O	N	E		S	I	R
2	B	C	D	F	G	H	J	K	L	M
6	P	Q	U	V	W	X	Y	Z		

   Listen to this short-wave radio broadcast from a numbers station, which reaches you as a special agent behind enemy lines. It contains a message which has been encoded by subtraction with the following key:

   66153 77185 10800 54937 48159 83271 12895 07132 34987 53954 23074

   Decrypt the message.