STANFORD SPLASH: CLASSICAL CIPHERS

NITYA MANI, ANDY CHEN

Cryptography Overview

As we have seen, Alice and Bob want to send each other messages, but they end up sending different messages from the ones they actually wanted to send. We will call the message they actually want to send the *plaintext*, and the message they actually send the *ciphertext*. A *cryptosystem* is a pair of algorithms, one to convert from a plaintext to a ciphertext, and the other to convert from a ciphertext back to a plaintext. In order to generate the ciphertext from the plaintext, two ingredients are needed: the protocol for encoding the message, and a specific *key*.

In the case of the Cæsar cipher, the Cæsar cipher is the protocol, and the key determines the size of the shift. In order to distinguish between the plaintext and the ciphertext, it is common to use uppercase letters for the ciphertext and lowercase letters for the plaintext. Sometimes, we will write the plaintext and ciphertext on two lines, as in the following:

Plaintext: `cryptography is fun`
Ciphertext `ETARVQITCRJA KU HWP`

Problems

(1) Generally, we use codes in order to prevent unwanted third parties from reading our messages. Are there any reasons why one might choose to write in code? Come up with as many as you can.

(2) Encrypt the message

`for duty, duty must be done; the rule applies to everyone.`

using a Cæsar cipher with a shift of 6 letters. (Don't worry about encrypting the punctuation.)

(3) The message

`ESTYRD LCP DPWOZX LD ESPJ DPPX.`

is a ciphertext encrypted using a Cæsar cipher (the shift amount is not provided). What is the plaintext message?

Date: April 10, 2016.

(4) Can you find two English words *other than* "sleep" and "bunny," with at least 4 letters, that encrypt to each other under a Cæsar cipher? What are the longest such words you can find?

(5) The following message has been encrypted with a substitution cipher: `GIUIFG CEI IPRC TPNN DU CEI QPRCNI`. Can you decrypt it? Do you have enough information from the decryption to determine the entire substitution table?

(6) Decrypt the message `HKPUFCMHY BHDDXZH` with the following simple substitution key:

Plaintext:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O

(7) The following message has been encyrpted using a substitution cipher: `D RNXHT VHRVCK VKKXOW FYVF V OVFY GENBWKKNE'K PWEC BVPNEDFW TWKKWEF DK GD.` Can you decrypt the message? Can you encrypt another message using the substitution table you discovered?

(8) (Challenge!) The message (with spaces removed)

```
NBPFR KISOQ NFRDB FKJFD XNOIN OJXIX NZXSI DJXIJ NYENO ISDSA SOFBY REJRK
IKSKI PFRAR DJZIJ RUSEE JXIZI KADFB JXIJK SODYI OGIOJ SEJIK ADSOG UESOJ
JXIAI VKPWX IKIPF RARDJ ENIRU FOJXI GSNDN IDSOG GNDYF RKDIN OOFVI EUXKS
DIDFB PFRKY FAUEN YSJIG DJSJI FBANO GJXIA ISONO ZGFID OJASJ JIKNB NJDFO
EPNGE IYXSJ JIKFB SJKSO DYIOG IOJSE LNOGS OGIVK PFOIW NEEDS PSDPF RWSEL
PFRKA PDJNY WSPNB JXNDP FROZA SOIQU KIDDI DXNAD IEBNO JIKAD JFFGI IUBFK
AIWXP WXSJS VIKPD NOZRE SKEPG IIUPF ROZAS OJXND GIIUP FROZA SOARD JCICI
IEFMR IOJNO UKSND IFBJX IVIKP GREEF EGGSP DWXNY XXSVI EFOZD NOYIU SDDIG
SWSPS OGYFO VNOYI IANBP FRYSO JXSJJ XIKIN ZOFBZ FFGMR IIOSO OIWSD YREJR
KIDUS EANID JGSPF BYFRK DIPFR WNEEU FFXUF FXWXS JIVIK DBKID XSOGO IWSOG
GIYES KINJD YKRGI SOGAI SOBFK SKJDJ FUUIG DXFKJ NOJXI YREJN VSJIG YFRKJ
FBJXI IAUKI DDHFD IUXNO ISOGI VKPFO IWNEE DSPSD PFRWS ELPFR KAPDJ NYWSP
NBJXS JDOFJ ZFFGI OFRZX BFKXN AWXNY XNDZF FGIOF RZXBF KAIWX PWXSJ SVIKP
YREJN VSJIG LNOGF BPFRJ XJXND LNOGF BPFRJ XARDJ CIJXI OSDIO JNAIO JSEUS
DDNFO FBSVI ZIJSC EIBSD XNFOA RDJIQ YNJIP FRKES OZRNG DUEII OSOSJ JSYXA
IOJSE SUESJ FBFKS CSDXB REPFR OZUFJ SJFFK SOFJJ FFBKI OYXBK IOYXC ISOJX
FRZXJ XIUXN ENDJN OIDAS PHFDJ EIPFR WNEEK SOLSD SOSUF DJEIN OJXIX NZXSI
DJXIJ NYCSO GNBPF RWSEL GFWOU NYYSG NEEPW NJXSU FUUPF KSENE PNOPF RKAIG
NIVSE XSOGS OGIVK PFOIW NEEDS PSDPF RWSEL PFRKB EFWKP WSPNB XIDYF OJIOJ
WNJXS VIZIJ SCEIE FVIWX NYXWF REGYI KJSNO EPOFJ DRNJA IWXPW XSJSA FDJUS
KJNYR ESKEP URKIP FROZA SOJXN DURKI PFROZ ASOAR DJCI
```

is a ciphertext encrypted using a substitution cipher. What is the plaintext message?