Symmetric Key Cryptography and Cryptographic Hashes Homework 2 solutions

John Manferdelli
jlm@cs.washington.edu
jmanfer@microsoft.com

Homework 1

Review DES description by reading

http://www.aci.net/kalliste/des.htm or

http://www.itl.nist.gov/fipspubs/fip46-2.htm

You need to know DES well for next class as well as for problem number 4.

Homework 1-Question 1

Encrypt the following message using a Vigeniere cipher with direct standard alphabets. Key: JOSH.

```
All persons born or naturalized in the United States, and
subject to the jurisdiction thereof, are citizens of the
United States and of the state wherein they reside. No
state shall make or enforce any law which shall abridge
the privileges or immunities of citizens of the United
States; nor shall any state deprive any person of life,
liberty, or property, without due process of law; nor deny
to any person within its jurisdiction the equal protection
of the laws.
```

Upper case only! Turn plain and cipher text into 5 letter groups.

Calculate the index of coincidence of the plaintext and ciphertext.

Break the ciphertext into 4 columns. What is the index of coincidence of each column?

Homework 1-Answer 1

```
ALLPE RSONS BORNO RNATU RALIZ EDINT HEUNI TEDST ATESA NDSUB JECTT
OTHEJ URISD ICTIO NTHER EOFAR ECITI ZENSO FTHEU NITED STATE SANDO
FTHES TATEW HEREI NTHEY RESID ENOST ATESH ALLMA KEORE NFORC EANYL
AWWHI CHSHA LLABR IDGET HEPRI VILEG ESORI MMUNI TIESO FCITI ZENSO
FTHEU NITED STATE SNORS HALLA NYSTA TEDEP RIVEA NYPER SONOF LIFEL
IBERT YORPR OPERT YWITH OUTDU EPROC ESSOF LAWNO RDENY TOANY PERSO
NWITH INITS JURIS DICTI ONTHE EQUAL PROTE CTION OFTHE LAWS
```

Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq
E	49	0.129	T	42	0.111	I	32	0.084	O	29	0.077
S	28	0.074	N	28	0.074	R	26	0.069	A	25	0.066
H	18	0.047	L	16	0.042	D	13	0.034	U	11	0.029
F	10	0.026	C	9	0.024	P	9	0.024	Y	8	0.021
W	7	0.018	B	4	0.011	M	3	0.008	J	3	0.008
Z	3	0.008	V	2	0.005	G	2	0.005	K	1	0.003
Q	1	0.003	X	0	0.000						

379 characters, index of coincidence: 0.069, IC (square approx): 0.071.

Homework 1-Answer 1 (cont)

```
JZDWN FKVWG TVABG YWOLB AODPI SVPWH ZLDBA ANRKA JHWZJ BVZDP BLLHL
VCVWQ DFAZM WUARC FAQSJ LXTSY NQAAR NWUBC XAQSM URHWK BHSAN GSUMC
XAQSK AJHWD QSJLR BLONM JLBWV LWCKA JHWZQ ODSVO CLXFW UOCJJ NOFFU
OODQW UOBVS SUOTY RRYLC VWWAW NPUSY LBCJP VAMUR HALBC XJRHA GNBKV
OHZLD BAANR KAJHW ZWCJZ QODSJ BQZCO LLMSH YRJWH WMHLA GGUXT DPOSD
PKSJA HCJWA CHLAH QDRHZ VDHVB NDJVL SKZXT DHFBG YMSFF CCSUH DWYBC
FDRHZ PWWLZ SIJPB RAJCW GUCVW LZISS YFGAN QLPXB GMCVW SJKK
```

Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq
W	29	0.077	A	28	0.074	S	23	0.061	L	23	0.061
J	22	0.058	H	22	0.058	C	20	0.053	B	20	0.053
D	18	0.047	V	17	0.045	O	15	0.040	Z	15	0.040
R	14	0.037	U	13	0.034	N	12	0.032	Q	12	0.032
F	11	0.029	K	11	0.029	P	10	0.026	G	10	0.026
Y	9	0.024	M	9	0.024	X	8	0.021	T	5	0.013
I	3	0.008	E	0	0.000		0	0.000			

379 characters, index of coincidence: 0.045, IC (square approx): 0.048

Homework 1-Answer 1 (cont further)

```
JNWAW AIWDN JJDLC DMRQX NRBQR BNMQJ QRNBW JQVXO
NUQBU RCAUB VRBRN ODNJW QJCMR WAXOK HAARD NLXFM
CHBRW SBCCZ YNXCJ
Column 1: 95 characters, index of coincidence: 0.058, IC (square approx):
      0.068.

ZFGBO OSHBR HBPHV FWCST QNCSH HGCSH SBMWC HOOFC
OOWVO RVWSC AHCHB HBRHC OBOSJ MGTSS CCHHH DSTBS
CDCHW IRWVI FQBVK
Column 2: 95 characters, index of coincidence: 0.077, IC (square approx):
      0.087.

DKTGL DVZAK WVBLW AUFJS AWXMW SSXKW JLJVK WDCWJ
FOUST YWNYJ MAXAK ZAKWJ DQLHW HGDDJ JHQZV JKDGF
SWFZL JAGWS GLGWK
Column 3: 95 characters, index of coincidence: 0.060, IC (square approx):
      0.070.

WVVYB PPLAA ZZLVQ ZAALY AUAUK AUAAD LOLLA ZSLUJ
FDOSY LWPLP ULJGV LAAZZ SZLYH LUPPA WLDVB VZHYF
UYDPZ PJULS APMS
Column4: 94 characters, index of coincidence: 0.081, IC (square approx): 0.090.
```

Homework 1-Question 2

Break the Vigeniere based ciphertext below. Plaintext and ciphertext alphabets are direct standard.

What is the key length? What is the key?

If the key length is k, how long a corresponding plain, ciphertext sequence be given to solve? Can you give an upper bound on the pure ciphertext length needed?

```
IGDLK MJSGC FMGEP PLYRC IGDLA TYBMR KDYVY XJGMR TDSVK ZCCWG ZRRIP
UERXY EEYHE UTOWS ERYWC QRRIP UERXJ QREWQ FPSZC ALDSD ULSWF FFOAM
DIGIY DCSRR AZSRB GNDLC ZYDMM ZQGSS ZBCXM OYBID APRMK IFYWF MJVLY
HCLSP ZCDLC NYDXJ QYXHD APRMQ IGNSU MLNLG EMBTF MLDSB AYVPU TGMLK
MWKGF UCFIY ZBMLC DGCLY VSCXY ZBVEQ FGXKN QYMIY YMXKM GPCIJ HCCEL
PUSXF MJVRY FGYRQ
```

Homework 1 - Answer 2

1	2	3	4	5	6	7	8	9	10	11	
IGDLK	MJSGC	FMGEP	PLYRC	IGDLA	TYBMR	KDYVY	XJGMR	TDSVK	ZCCWG	ZRRIP	1
UERXY	EEYHE	UTOWS	ERYWC	QRRIP	UERXJ	QREWQ	FPSZC	ALDSD	ULSWF	FFOAM	2
DIGIY	DCSRR	AZSRB	GNDLC	ZYDMM	ZQGSS	ZBCXM	OYBID	APRMK	IFYWF	MJVLY	3
HCLSP	ZCDLC	NYDXJ	QYXHD	APRMQ	IGNSU	MLNLG	EMBTF	MLDSB	AYVPU	TGMLK	4
MWKGF	UCFIY	ZBMLC	DGCLY	VSCXY	ZBVEQ	FGXKN	QYMIY	YMXKM	GPCIJ	HCCEL	5
PUSXF	MJVRY	FGYRQ									

First Repetition: 20, Second: 25. Third: 53. (20,25,35)=5

ALDSD	FFOAM	IFYWF	NYDXJ	UCFIY	ZBCXM
APRMK	FGXKN	IGDLA	OYBID	UERXJ	ZBMLC
APRMQ	FGYRQ	IGDLK	PLYRC	UERXY	ZBVEQ
AZSRB	FMGEP	IGNSU	PUSXF	ULSWF	ZCCWG
DCSRR	FPSZC	KDYVY	QREWQ	UTOWS	ZCDLC
DGCLY	GNDLC	MJSGC	QRRIP	VSCXY	ZQGSS
DIGIY	GPCIJ	MJVLY	QYMIY	XJGMR	ZRRIP
EEYHE	HCCEL	MJVRY	QYXHD	YMXKM	ZYDMM
EMBTF	HCLSP	MLDSB	TDSVK	YVPU	
ERYWC		MLNLG	TGMLK		
		MWKGF	TYBMR		

Homework 1-Answer 2 (cont)

Full Cipher

Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq
Y	23	0.079	M	21	0.072	C	19	0.066	R	18	0.062
G	17	0.059	L	16	0.055	D	16	0.055	S	15	0.052
F	13	0.045	I	12	0.041	P	11	0.038	E	11	0.038
X	10	0.034	Z	10	0.034	Q	9	0.031	B	8	0.028
K	8	0.028	U	8	0.028	W	7	0.024	A	7	0.024
J	7	0.024	V	7	0.024	N	5	0.017	T	5	0.017
H	4	0.014	O	3	0.010		0	0.000			

290 characters, index of coincidence: 0.044, IC (square approx): 0.047.

Column 1 of 5

Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq
Z	8	0.138	M	6	0.103	A	5	0.086	U	5	0.086
F	5	0.086	I	4	0.069	Q	4	0.069	T	3	0.052
D	3	0.052	E	3	0.052	H	2	0.034	P	2	0.034
G	2	0.034	O	1	0.017	K	1	0.017	V	1	0.017
X	1	0.017	Y	1	0.017	N	1	0.017	S	0	0.000
B	0	0.000	C	0	0.000	J	0	0.000	W	0	0.000
L	0	0.000	R	0	0.000		0	0.000			

58 characters, index of coincidence: 0.059, IC (square approx): 0.075.

Homework 1-Answer 2 (cont)

Column 2 of 5

Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq
G	7	0.121	Y	7	0.121	C	6	0.103	L	5	0.086
P	4	0.069	R	4	0.069	J	4	0.069	E	3	0.052
B	3	0.052	M	3	0.052	F	2	0.034	D	2	0.034
Q	1	0.017	N	1	0.017	S	1	0.017	T	1	0.017
U	1	0.017	W	1	0.017	I	1	0.017	Z	1	0.017
O	0	0.000	K	0	0.000	V	0	0.000	H	0	0.000
X	0	0.000	A	0	0.000		0	0.000			

58 characters, index of coincidence: 0.058, IC(square approx): 0.074.

Column 3 of 5

Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq
D	8	0.138	S	7	0.121	R	6	0.103	C	6	0.103
Y	6	0.103	V	4	0.069	G	4	0.069	B	3	0.052
X	3	0.052	M	3	0.052	O	2	0.034	N	2	0.034
F	1	0.017	E	1	0.017	K	1	0.017	L	1	0.017
P	0	0.000	Q	0	0.000	A	0	0.000	T	0	0.000
U	0	0.000	H	0	0.000	W	0	0.000	I	0	0.000
J	0	0.000	Z	0	0.000		0	0.000			

58 characters, index of coincidence: 0.071, IC (square approx): 0.087.

Homework 1-Answer 2 (cont)

Column 4 of 5

Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq
L	9	0.155	I	7	0.121	W	6	0.103	X	6	0.103
S	5	0.086	M	5	0.086	R	5	0.086	E	3	0.052
H	2	0.034	V	2	0.034	G	2	0.034	K	2	0.034
A	1	0.017	P	1	0.017	T	1	0.017	Z	1	0.017
C	0	0.000	Q	0	0.000	D	0	0.000	J	0	0.000
U	0	0.000	F	0	0.000	B	0	0.000	N	0	0.000
Y	0	0.000	O	0	0.000		0	0.000			

58 characters, index of coincidence: 0.075, IC (square approx): 0.091.

Column 5 of 5

Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq	Ch	Count	Freq
Y	9	0.155	C	7	0.121	F	5	0.086	M	4	0.069
P	4	0.069	Q	4	0.069	K	4	0.069	J	3	0.052
R	3	0.052	D	3	0.052	G	2	0.034	S	2	0.034
U	2	0.034	B	2	0.034	A	1	0.017	N	1	0.017
E	1	0.017	L	1	0.017	H	0	0.000	O	0	0.000
T	0	0.000	I	0	0.000	V	0	0.000	W	0	0.000
X	0	0.000	Z	0	0.000		0	0.000			

58 characters, index of coincidence: 0.063, IC (square approx): 0.079.

Homework 1-Answer 2 (cont)

Side normal alphabet against input alphabet and check distance:

$D_i = \sum_{i=0}^{25} (d_i - d'_{((i+s)(\mathrm{mod}\ 26))})^2$. d_i is the cipher alphabet frequency, d_i' is the normal alphabet frequency.

Alphabet 1 Slide	Distance	Alphabet 1 Slide	Distance	Alphabet 2 Slide	Distance	Alphabet 2 Slide	Distance
00 (A)	0.0656	13 (N)	0.0707	00 (A)	0.0724	13 (N)	0.0494
01 (B)	0.0556	14 (O)	0.0791	01 (B)	0.0733	14 (O)	0.0724
02 (C)	0.0703	15 (P)	0.0723	02 (C)	0.0540	15 (P)	0.0636
03 (D)	0.0753	16 (Q)	0.0603	03 (D)	0.0795	16 (Q)	0.0689
04 (E)	0.0704	17 (R)	0.0621	04 (E)	0.0712	17 (R)	0.0691
05 (F)	0.0775	18 (S)	0.0736	05 (F)	0.0649	18 (S)	0.0693
06 (G)	0.0616	19 (T)	0.0700	06 (G)	0.0730	19 (T)	0.0702
07 (H)	0.0619	20 (U)	0.0693	07 (H)	0.0645	20 (U)	0.0446
08 (I)	0.0401	21 (V)	0.0440	08 (I)	0.0785	21 (V)	0.0752
09 (J)	0.0896	22 (W)	0.0679	09 (J)	0.0625	22 (W)	0.0777
10 (K)	0.0899	23 (X)	0.0704	10 (K)	0.0701	23 (X)	0.0732
11 (L)	0.0666	24 (Y)	0.0816	11 (L)	0.0404	**24 (Y)**	**0.0135**
12 (M)	**0.0163**	25 (Z)	0.0553	12 (M)	0.0784	25 (Z)	0.0754

Homework 1-Answer 2 (cont)

Side normal alphabet against input alphabet and check distance:

$D_i = \sum_{i=0}^{25} (d_i - d'_{((i+s)(\mathrm{mod}\ 26))})^2$. d_i is the cipher alphabet frequency, d_i' is the normal alphabet frequency.

Alphabet 3 Slide		Distance	Alphabet 3 Slide		Distance	Alphabet 4 Slide		Distance	Alphabet 4 Slide		Distance
00	(A)	0.0764	13	(N)	0.0647	00	(A)	0.0711	13	(N)	0.0929
01	(B)	0.0901	14	(O)	0.0599	01	(B)	0.1091	14	(O)	0.0839
02	(C)	0.0841	15	(P)	0.0763	02	(C)	0.1079	15	(P)	0.0734
03	(D)	0.0836	16	(Q)	0.0838	03	(D)	0.0672	16	(Q)	0.1000
04	(E)	0.0744	17	(R)	0.0799	**04**	**(E)**	**0.0231**	17	(R)	0.0759
05	(F)	0.0823	18	(S)	0.0907	05	(F)	0.0829	18	(S)	0.0577
06	(G)	0.0849	19	(T)	0.0871	06	(G)	0.0878	19	(T)	0.0508
07	(H)	0.0960	20	(U)	0.0741	07	(H)	0.0751	20	(U)	0.0782
08	(I)	0.0966	21	(V)	0.0752	08	(I)	0.0675	21	(V)	0.0949
09	(J)	0.0718	22	(W)	0.1086	09	(J)	0.0893	22	(W)	0.0971
10	**(K)**	**0.0338**	23	(X)	0.0919	10	(K)	0.0924	23	(X)	0.0860
11	(L)	0.0755	24	(Y)	0.0494	11	(L)	0.0896	24	(Y)	0.0832
12	(M)	0.0917	25	(Z)	0.0426	12	(M)	0.1074	25	(Z)	0.0876

Homework 1-Answer 2 (cont)

Side normal alphabet against input alphabet and check distance:

$D_i = \sum_{i=0}^{25} (d_i - d'_{((i+s)(\mathrm{mod}\ 26))})^2$. d_i is the cipher alphabet frequency, d_i' is the normal alphabet frequency.

Alphabet 5 Slide	Distance
00 (A)	0.0900
01 (B)	0.0696
02 (C)	0.0624
03 (D)	0.0871
04 (E)	0.0888
05 (F)	0.0598
06 (G)	0.0763
07 (H)	0.0732
08 (I)	0.0833
09 (J)	0.0663
10 (K)	0.0593
11 (L)	0.0539
12 (M)	0.0599

Alphabet 5 Slide	Distance
13 (N)	0.0684
14 (O)	0.0759
15 (P)	0.0846
16 (Q)	0.0613
17 (R)	0.0724
18 (S)	0.0806
19 (T)	0.0889
20 (U)	0.0466
21 (V)	0.0833
22 (W)	0.0781
23 (X)	0.0661
24 (Y)	**0.0215**
25 (Z)	0.0699

Homework 1-Answer 2 (cont)

Vig Tableau

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
--------------------------
MNOPQRSTUVWXYZABCDEFGHIJKL
YZABCDEFGHIJKLMNOPQRSTUVWX
KLMNOPQRSTUVWXYZABCDEFGHIJ
EFGHIJKLMNOPQRSTUVWXYZABCD
YZABCDEFGHIJKLMNOPQRSTUVWX
```

Homework 1-Answers 2

```
WITHM ALICE TOWAR DNONE WITHC HARIT YFORA LLWIT
HFIRM NESSI NTHER IGHTA SGODG IVESU STOSE ETHER
IGHTL ETUSS TRIVE ONTOF INISH THEWO RKWEA REINT
OBIND UPTHE NATIO NSWOU NDSTO CAREF ORHIM WHOSH
ALLHA VEBOR NETHE BATTL EANDF ORHIS WIDOW ANDHI
SORPH ANTOD OALLW HICHM AYACH IEVEA NDCHE RISHA
JUSTA NDLAS TINGP EACEA MONGO URSEL VESAN DWITH
ALLNA TIONS

Key Length: 5
Key: MYKEY
```

Corresponding plain/cipher required: k.

Cipher only< 25k [assuming 25 letters are required to identify one letter with high certainty, a pretty conservative assumption. You could argue it was as small as about 8k.].

Homework 1-Question 3

Consider a message source M(x) with the following distribution:

M: P(x=0)= p

M: P(x=1)= q, with p+q=1

and a one time pad selected from distribution P(x)

P: P(x=0)= ½

P: P(x=1)= ½

Consider the ciphertext formed by "xoring" the message m with the pad p, so that c= m⊕p

What is the ciphertext distribution C?

Calculate H(M), H(P), H(C).

Calculate: I(M|C)= H(M)-H(M|C)

Suppose, P: P(x=0)=3/4 and P(x=1)=1/4. What is the ciphertext distribution and H(M), H(P), H(C) and I(M|C) now.

Homework 1-Answer 3

P(c=0)= P(m=0)P(p=0)+P(m=1)P(p=1)= p(1/2)+q(1/2)= 1/2

P(c=1)= P(m=1)P(p=0)+P(m=0)P(p=1)= p(1/2)+q(1/2)= 1/2

H(M)= -p lg(p) – q lg(q)

H(P)= -1/2 lg(1/2) – 1/2 lg(1/2)= 1 (bit)

H(C)= 1 (bit)

H(M,C)= P(M=0,C=0) lg(P(M=0,C=0))+P(M=0,C=1) lg(P(M=0,C=1))+
P(M=1,C=0) lg(P(M=1,C=0))+P(M=1,C=1) lg(P(M=1,C=1))

P(M=0,C=0)= p/2, etc

I(M|C)= H(M) – H(M|C)= H(M)+H(C) – H(M,C)

I(M|C)= -p lg(p) – q lg(q) +1 + p/2 lg(p/2) + q/2 lg(q/2) + p/2 lg(p/2) + q/2 lg(q/2) = -p lg(p) –q lg(q) +1 +p lg(p/2)+q(lg(q/2)=0

Homework 1-Answer 3 (cont)

P(c=0)= P(m=0)P(p=0)+P(m=1)P(p=1)= p(3/4)+q(1/4)= (3p+q)/4
P(c=1)= P(m=1)P(p=0)+P(m=0)P(p=1)= p(1/4)+q(3/4)= (3q+p)/4
H(M)= -p lg(p) – q lg(q)
H(P)= -3/4 lg(3/4) – 1/4 lg(1/4) $\approx$ .81 (bit)
H(C)= -(3p+q)/4 lg((3p+q)/4) -(3q+p)/4 lg((3q+p)/4)

H(M,C)= P(M=0,C=0) lg(P(M=0,C=0))+P(M=0,C=1) lg(P(M=0,C=1))+
P(M=1,C=0) lg(P(M=1,C=0))+P(M=1,C=1) lg(P(M=1,C=1))
P(M=0,C=0)= 3p/4, P(M=0,C=1)= p/4, P(M=1,C=0)= 3q/4, P(M=1,C=1)= q/4,

I(M|C)= H(M) – H(M|C)=H(M)+H(C) –H(M,C)
I(M|C)= -p lg(p) – q lg(q) -(3p+q)/4 lg((3p+q)/4) -(3q+p)/4 lg((3q+p)/4)+
3p/4 lg(3p/4)+p/4 lg(p/4)+3q/4 lg(3q/4)+q/4 lg(q/4)=
-(3p+q)/4 lg((3p+q)/4) -(3q+p)/4 lg((3q+p)/4)+ 3/4 lg(3/4) + 1/4 lg(1/4) $\approx$
-(3p+q)/4 lg((3p+q)/4) -(3q+p)/4 lg((3q+p)/4)-.80
Note: If you didn't simplify, it's OK

Homework 1-Question 4

Calculate the output of the first two rounds of DES with input message ~~0x3132333435363738~~ 0x3433323138373635. The input to round 1 (after initial permutation) and the first 2 round keys are given below.

For fixed key, DES is a permutation on 2^{64} letters.

Approximately how many such permutations are there? (Hint: Use Stirling's approximation.)

Compare this to the size of the key space for DES.

```
Round 01 Key:    01001111 01010111 00000111 10111001 01011100 10101011
Round 02 Key:    00101111 00100111 01101001 00111011 01111111 00100100

Input to DES:    00110100 00110011 00110010 00110001
                 00111000 00110111 00110110 00110101
Round 1 Input:   00000000 11111111 11100001 10101010
                 00000000 11111111 00010000 01100110
```

Homework 1-Answer4

```
KEY: 0xabcdef89abcdef89
DES Input: desin.txt, Output: desout.bin, Key: 00abcdefabcdef89,

Round 01 Key:  01001111 01010111 00000111 10111001 01011100 10101011
Round 02 Key:  00101111 00100111 01101001 00111011 01111111 00100100
Round 03 Key:  11001011 01010100 10111001 10111000 01001001 10110010
Round 04 Key:  11011101 10001011 11011000 11000101 01101010 00010111
Round 05 Key:  00010110 11111010 10001011 11110111 00100010 11011000
Round 06 Key:  00111011 00111101 01000110 10110001 10010011 01001111
Round 07 Key:  01101000 01101100 11001101 00010110 10110110 10100110
Round 08 Key:  01010001 11100101 00111100 01111100 00101101 11100101
Round 09 Key:  11010110 11001100 11101100 01100110 11110000 10100101
Round 10 Key:  11011010 11100011 00100010 11100010 00101101 11101011
Round 11 Key:  10101000 10011111 00101111 10101110 10011011 00011011
Round 12 Key:  11100001 00110010 01001111 01010111 01010111 01110010
Round 13 Key:  00100001 11011110 11110000 01011101 10001001 01101000
Round 14 Key:  11010100 01111001 11110010 11000000 11111100 01011100
Round 15 Key:  10110110 11100111 01010001 01101001 10110110 10111100
Round 16 Key:  10101110 01111001 00010111 10001010 11110110 00111001
```

Homework 1-Answer 4 (cont)

```
Input to DES:        00110100 00110011 00110010 00110001
                     00111000 00110111 00110110 00110101
After IP:            00000000 11111111 11100001 10101010
                     00000000 11111111 00010000 01100110

Round 01  f:         00100101 00001011 10111110 11110100
After round 01:      00000000 11111111 00010000 01100110
                     00100101 11110100 01011111 01011110

Round 02  f:         10000000 00110000 00111001 11101111
After round 02:      00100101 11110100 01011111 01011110
                     10000000 11001111 00101001 10001001
```

Homework 1-Answer 4 (cont)

Stirling: $N! \approx \sqrt{(2 \pi N)}\ (N/e)^N$

$N = 2^{64} \approx 16 \times 10^{18}$. $[2^{10}=1024 \approx 10^3.]$

Look at $R=N!/2^{56}$, the ratio of the sizes. Let $r = \ln(R)$.

$r = \frac{1}{2} \ln(2 \pi N) + N \ln(N/e) - 56 \ln(2)$. $r \approx \frac{1}{2}(1+45) - 39 + 16 \times 10^{18} (64 \ln(2) - 1) \approx 16 \times 10^{18}\ 64 \ln(2) \approx 7 \times 10^{20}$.

$R = \exp(7 \times 10^{20})$, an unfathomably large number.

You may have "rounded" differently or expressed the answer as a power of 2. That's OK.

Homework 1-Answer 4 (Addendum)

```
Round 1 Input:     L: 00000000 11111111 11100001 10101010
                   R: 00000000 11111111 00010000 01100110

010011 110101 011100 000111 101110 010101 110010 101011  K1
000000 000001 011111 111110 100010 100000 001100 001100  E(R)
010011 110100 000011 111001 001100 110101 111110 100111  K⊕E(R)
1/1001 2/1010 1/0001 3/1100 0/0110 3/1010 2/1111 3/0011  Row/Indx
6      c      7      c      b      1      2      7       S box out
0110   1100   0111   1100   1011   0001   0010   0111    As Bits
0010   0101   0000   1011   1011   1110   1111   0100    Apply P

00100101 00001011 10111110 11110100    f(K1,R)
00000000 11111111 11100001 10101010    L
00100101 11110100 01011111 01011110    L⊕f(K1,R)
Output: R||L⊕f(K1,R)

Round 1 Output:       00000000 11111111 00010000 01100110
                      00100101 11110100 01011111 01011110
```

Homework 1-Question 5

Given a one rotor machine, M, depicted below with equation ~~$C^i R^{-1} C^{-i} U C^{-i} R C^i (p)=c$~~, $C^{-i} R^{-1} C^i U C^{-i} R C^i (p_i)=c_i$ with C, U, R below.

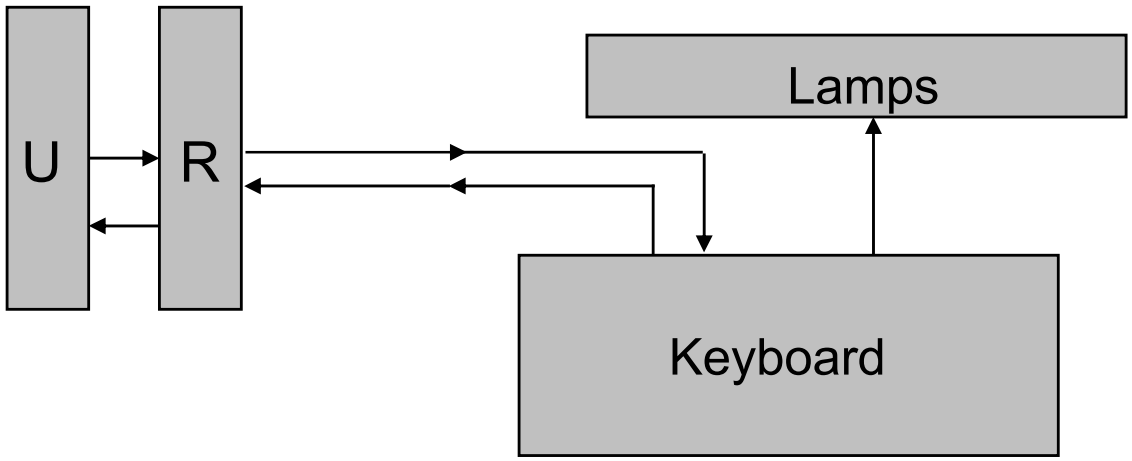
R: ABCDEFGHIJKLMNOPQRSTUVWXYZ

EKMFLGDQVZNTOWYHXUSPAIBRCJ

U: ABCDEFGHIJKLMNOPQRSTUVWXYZ

YRUHQSLDPXNGOKMIEBFZCWVJAT

C: The cyclic permutation A→B, B→C, etc



Homework 1-Question 5 (cont)

Calculate the ciphertext derived from the plaintext: `HELLOWORLD`

What do you think the index of coincidence of the ciphertext

from a 50 letter message is?

If the key was the "starting position," i=0 (if you started at i=1, it's OK), of M, how many letters

of corresponding plain/cipher text would you need to find the key? How many ciphertext only letters?

The following may be helpful:

R^{-1} `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

`UWYGADFPVZBECKMTHXSLRINQOJ`

Homework 1-Answer 5 (as asked)

$C^i\ R^{-1}\ C^{-i}\ U\ C^{-i}\ R\ C^i\ (p)=c$

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

Note: Some people started at i=1, since the question was ambiguous, that's acceptable.

Homework 1-Answer 5 (correct)

$C^{-i}\ R^{-1}\ C^{i}\ U\ C^{-i}\ R\ C^{i}\ (p)=c$

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

Homework 1-Answer 5 (correct)

IC for 50 letters: about .038 since there are 26 alphabets

Required corresponding plain/chosen: 1 or 2 (depends on input). Saying "a few" or even 1 letter would be acceptable here.

Explanation:

The "key" is the starting position of the rotor (i). If you have a single plain/cipher pair, say p and c, you can find an i such that

$C^{-i}\ R^{-1}\ C^{i}\ U\ C^{-i}\ R\ C^{i}\ (p)=c$.

Sometimes a few i's will work because $C^{-i}\ C^{-i}\ R^{-1}\ C^{i}\ U\ C^{-i}\ R\ C^{i}\ (p)= C^{-j}\ R^{-1}\ C^{j}\ U\ C^{-j}\ R\ C^{j}\ (p)$ can have solutions for i!=j. So sometimes you need another letter to disambiguate. [A full explanation is very hard and probabilistic in nature.]

Ciphertext only: about 30.

Homework 1-Question 5

Given a one rotor machine, M, depicted below with equation ~~$C^{i}\ R^{-1}\ C^{-i}\ U\ C^{-i}\ R\ C^{i}\ (p)=c$~~, $C^{-i}\ R^{-1}\ C^{i}\ U\ C^{-i}\ R\ C^{i}\ (p)=c$ with C, U, R below.

R: ABCDEFGHIJKLMNOPQRSTUVWXYZ
EKMFLGDQVZNTOWYHXUSPAIBRCJ

U: ABCDEFGHIJKLMNOPQRSTUVWXYZ
YRUHQSLDPXNGOKMIEBFZCWVJAT

C: The cyclic permutation:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

R^{-1} ABCDEFGHIJKLMNOPQRSTUVWXYZ
UWYGADFPVZBECKMTHXSLRINQOJ