Kapitel 2

2.1 a) $c = am + b \Rightarrow m = a^{-1}(c - b)$.

b) a has to have an inverse in $\mathbb{Z}_{26}$. The number of possible choices for a is $\phi(26) = \phi(2)\phi(13) = 1 \cdot 12 = 12$. Hence the number of possible keys is $12 \cdot 26 = 312$.

2.3 We have a Vigenère cipher. We start by determining the period and we are interested in substrings that occur more than once. We find the distance between two substrings that are equal. The substrings are given below with the distance in paranthesis.

```
AM(196) AS(175) DP(36)(60)(96) EE(4) EJ(69)(146)(215) EJK(215) EX(100)
FM(12)(20)(30)(32)(50)(57)(62)(128)(140)(160)(185)(190)(197)(217)(247) FMPZJNVC(160) GK(14)(71)(85)
HY(125) IG(53)(87)(90)(143)(177)(230) IO(17) IZ(20)(45)(125)(145)(170)(190) JA(60) JK(215) JNVC(160)
JZXIG(90) KH(55) KI(86) KQ(37) KU(119) LA(65)(75)(140) LL(10)(11) LUFMPZJNVC(160) LX(149) MI(11)(12)(23)
MJ(50) MPZJNVC(160) MW(195) MZ(182) NL(45)(105)(150) NV(12)(160)(172) NVC(160) OI(2) PL(115)
PT(24)(50)(74) PTE(50) PV(84) PZJNVC(160) QGK(85) QL(111) TE(50) TI(160) UA(163) UFMPZJNVC(160) UKH(55)
VC(160) VI(103) VX(20) WF(33) WP(36)(118)(154) XE(49)(69)(118) XI(40)(90)(130) XIG(90) YM(25) ZI(58)
ZJNVC(160) ZLA(65) ZV(81) ZXIG(90)
```

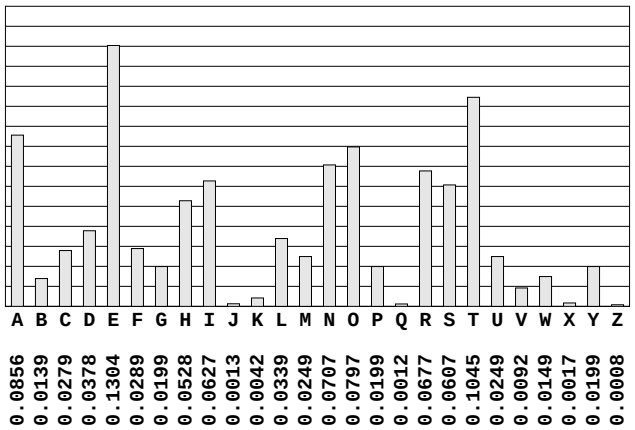
If we factor all distances we see that there are several candidates to the period length. The dominating factor is 5 so this is the one we will try with. The relative frequencies in the English alphabet is given as

$$A = (\alpha_0, \alpha_1, \ldots, \alpha_{25}),$$

see table. This means that the probability that a letter is a `C` is given by $\alpha_2 = 0.0279$.
We shall also find the symbol frequencies for 5 alphabets B_0, B_1, B_2, B_3 and B_4. The alphabet B_0 is given by the symbols at positions 0, 5, 10 and so on in the ciphertext. We will write them as

$$(\beta_0^0, \beta_1^0, \ldots, \beta_{25}^0).$$

Symbol probabilities for the English alphabet



Corresponding distributions exists for the other 4 alphabets. Each distribution is to be tested against the distribution above in order to find the most probable shift in each position. To get a quantitative measurement of how probable a certain shift is we use the following metric.

$$t_r = \sum_{i=0}^{25} (\alpha_i - \beta_{i+r \pmod{26}})^2; r = 0, 1, \ldots, 25$$

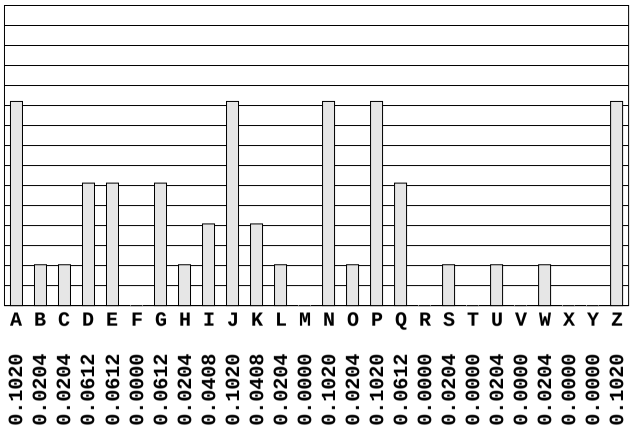
The most probable shift is then given by minimizing over all possible shifts, i.e.,

$$\min_r t_r$$

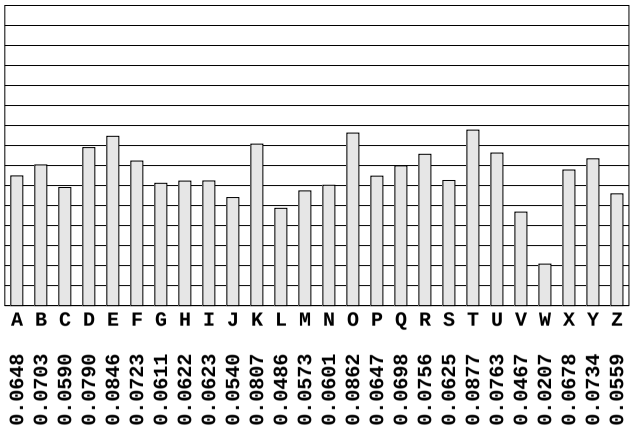
will give a probable shift $r_{\min}$.

For the different key positions we now give the symbol frequencies and t_r for different values of r. When $r = 0$ we write an `A`, for $r = 1$ a `B`, and so on.

Symbol frequencies for B_0 $(\beta_0^0, \beta_1^0, \ldots, \beta_{25}^0)$.

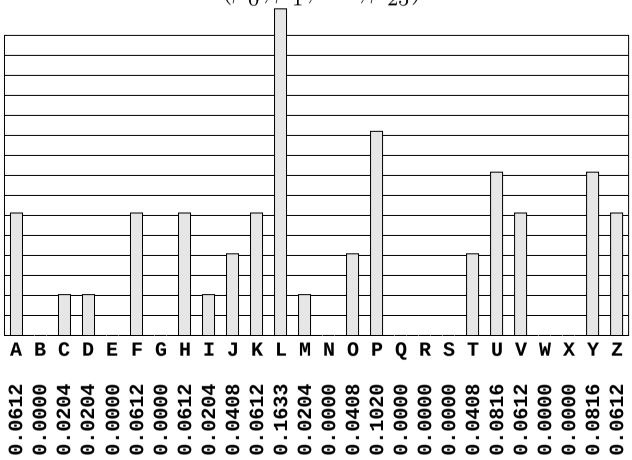


t_r for given $(\beta_0^0, \beta_1^0, \ldots, \beta_{25}^0)$.

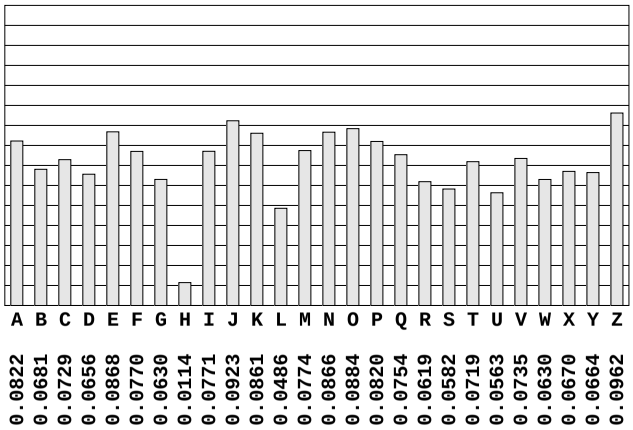


From this we draw the conclusion that `W` is the first key symbol.

Symbol frequencies for B_1 $(\beta_0^1, \beta_1^1, \ldots, \beta_{25}^1)$.

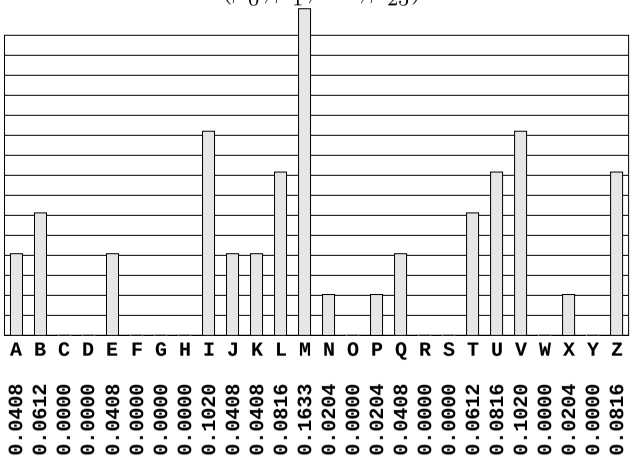


t_r for given $(\beta_0^1, \beta_1^1, \ldots, \beta_{25}^1)$.

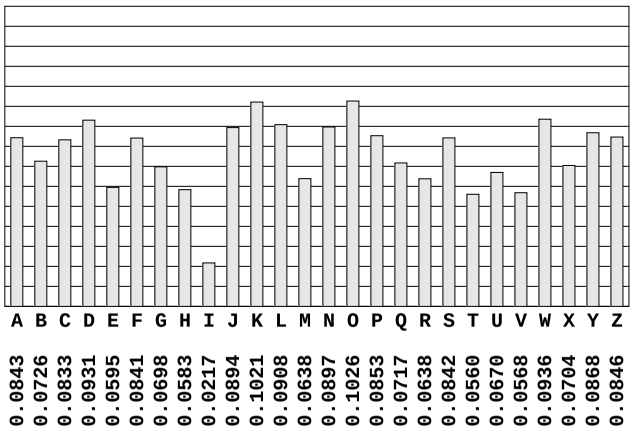


From this we draw the conclusion that `H` is the second key symbol.

Symbol frequencies for B_2 $(\beta_0^2, \beta_1^2, \ldots, \beta_{25}^2)$.

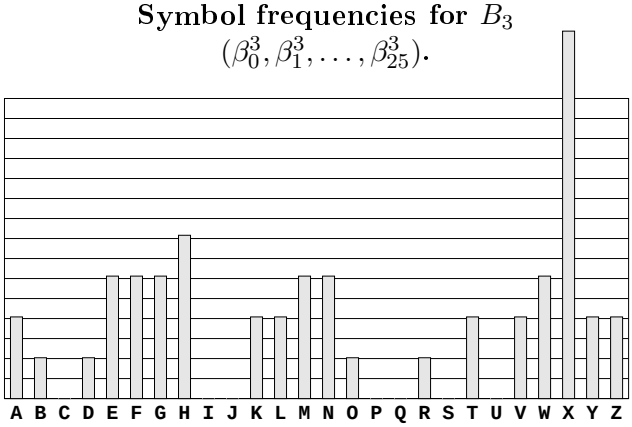


t_r for given $(\beta_0^2, \beta_1^2, \ldots, \beta_{25}^2)$.



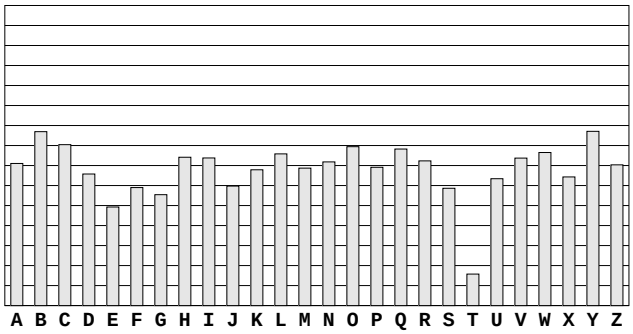
From this we draw the conclusion that `I` is the third key symbol.

Symbol frequencies for B_3 $(\beta_0^3, \beta_1^3, \ldots, \beta_{25}^3)$.



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
0.0408	0.0204	0.0000	0.0204	0.0612	0.0612	0.0612	0.0816	0.0000	0.0000	0.0408	0.0408	0.0612	0.0612	0.0204	0.0000	0.0000	0.0204	0.0000	0.0408	0.0000	0.0408	0.0612	0.1837	0.0408	0.0408

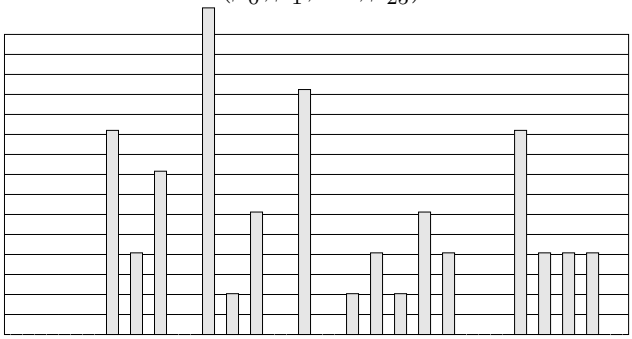
t_r for given $(\beta_0^3, \beta_1^3, \ldots, \beta_{25}^3)$.



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
0.0710	0.0869	0.0804	0.0658	0.0493	0.0590	0.0554	0.0741	0.0738	0.0597	0.0679	0.0758	0.0687	0.0718	0.0794	0.0691	0.0782	0.0723	0.0586	0.0157	0.0634	0.0737	0.0765	0.0643	0.0871	0.0704

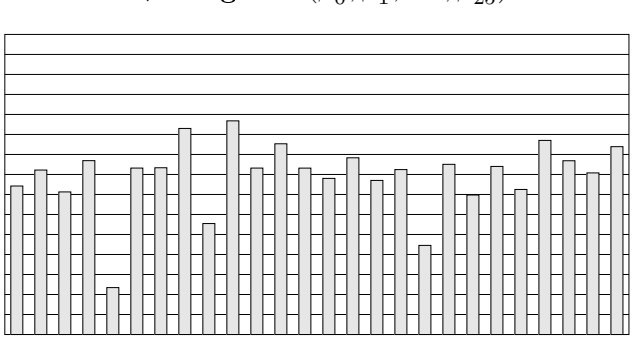
From this we draw the conclusion that `T` is the fourth key symbol.

Symbol frequencies for B_4 $(\beta_0^4, \beta_1^4, \ldots, \beta_{25}^4)$.



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
0.0000	0.0000	0.0000	0.0000	0.1020	0.0408	0.0816	0.0000	0.1633	0.0204	0.0612	0.0000	0.1224	0.0000	0.0204	0.0408	0.0204	0.0612	0.0408	0.0000	0.0000	0.1020	0.0408	0.0408	0.0408	0.0000

t_r for given $(\beta_0^4, \beta_1^4, \ldots, \beta_{25}^4)$.



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
0.0742	0.0822	0.0713	0.0869	0.0234	0.0832	0.0834	0.1030	0.0555	0.1068	0.0832	0.0953	0.0832	0.0780	0.0883	0.0770	0.0824	0.0445	0.0851	0.0697	0.0840	0.0725	0.0970	0.0869	0.0808	0.0939

From this we draw the conclusion that `E` is the fifth key symbol.

This gives the following plain text:

```
ENCOU NTERE DREDI NFANT RYEST IMATE DATON EREGI MENTA NDMAC HINEG UNCOM PANYI NTRUC
KSNEA REMMI TSBUR GAMHO LDING MIDDL ECREE KNEAR HILLF IVEFO URTHR EESOU THWES TOFFA
IRPLA YWHEN FORCE DBACK WILLC ONTIN UEDEL AYING REDSA TMARS HCREE KHAVE DESTR OYEDB
RIDGE SONMI DDLEC REEKB ETWEE NEMMI TSBUR GTANE YTOWN ROADA NDRHO DESMI LL
```

2.5 The number of possible keys is the number of invertible matrices in $\mathbb{Z}_{26}$. Using the chinese remainder theorem we know that $\mathbb{Z}_{26}$ can be represented as $\mathbb{Z}_2 \times \mathbb{Z}_{13}$. Thus, we need to find the number of invertible matrices in $\mathbb{Z}_2$ and $\mathbb{Z}_{13}$. The number of invertible matrices is equivalent to the number of ways we can write a matrix with linearly independent rows.

$t = 2$: There are $(2^2 - 1) \cdot (2^2 - 2) = 6$ invertible matrices in $\mathbb{Z}_2$. There are $(13^2 - 1) \cdot (13^2 - 13) = 26208$ invertible matrices in $\mathbb{Z}_{13}$. Thus, there are in total $6 \cdot 26208 = 157248$ invertible 2×2 matrices in $\mathbb{Z}_{26}$

$t = 3$: There are $(2^3 - 1) \cdot (2^3 - 2) \cdot (2^3 - 2^2) = 168$ invertible matrices in $\mathbb{Z}_2$. There are $(13^3 - 1) \cdot (13^3 - 13) \cdot (13^3 - 13^2) = 9726417792$ invertible matrices in $\mathbb{Z}_{13}$. Thus, there are in total $168 \cdot 9726417792 = 1634038189056 \approx 2^{40.6}$ invertible 3×3 matrices in $\mathbb{Z}_{26}$.

Kapitel 3

3.1 a) $H(W) = -\sum_w f_W(w) \log f_W(w)$; $H(W|V) = \sum_v f_V(v) H(W|V = v)$.

1. $H(X) = H(\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}) = -6 \cdot (\frac{1}{6} \log \frac{1}{6}) = \log 6 \approx 2.585$.
2. $H(Y) = H(\frac{1}{2}, \frac{1}{2}) = h(\frac{1}{2}) = -\frac{1}{2} \log \frac{1}{2} - \frac{1}{2} \log \frac{1}{2} = \log 2 = 1$.
3. $H(Z) = H(\frac{1}{2}, \frac{1}{2}) = 1$.

4. $H(XY) = H(0, \frac{1}{6}, \frac{1}{6}, 0, 0, \frac{1}{6}, \frac{1}{6}, 0, 0, \frac{1}{6}, \frac{1}{6}, 0) = H(\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}) = \log 6 \approx 2.585$.
   Alternatively: $H(XY) = H(X) + H(Y|X)$;
   $H(Y|X) = 0$: when we know X, we also know Y. Så $H(XY) = \log 6 + 0 = \log 6 \approx 2.585$.
5. $H(XZ) = H(X) + H(Z|X) = \log 6 + 0 = \log 6$.
6. $H(YZ) = H(Y) + H(Z|Y)$;
   $H(Z|Y) = \frac{1}{2}H(Z|Y = \text{ODD}) + \frac{1}{2}H(Z|Y = \text{EVEN}) = \frac{1}{2}H(\frac{2/6}{3/6}, \frac{1/6}{3/6}) + \frac{1}{2}H(\frac{1/6}{3/6}, \frac{2/6}{3/6}) = \frac{1}{2}h(\frac{1}{3}) + \frac{1}{2}h(\frac{1}{3}) = h(\frac{1}{3}) = -\frac{2}{3} + \log 3$.
   Så $H(YZ) = 1 + h(\frac{1}{3}) = \frac{1}{3} + \log 3 \approx 1.918$.
7. $H(XYZ) = H(X) + H(YZ|X) = \log 6 + 0 = \log 6$.

b) $I(V;W) = \sum_v \sum_w f_{VW}(v,w) \log \frac{f_{V|W}(v|w)}{f_V(v)} = H(V) - H(V|W) = H(W) - H(W|V)$.

1. $I(X;Y) = H(Y) - H(Y|X) = 1 - 0 = 1$.
2. $I(X;Z) = H(Z) - H(Z|X) = 1 - 0 = 1$.
3. $I(Y;Z) = H(Y) + H(Z) - H(YZ) = 1 + 1 - (1 + h(\frac{1}{3})) = \frac{5}{3} - \log 3 \approx 0.0817$.
4. $I(X;YZ) = H(YZ) - H(YZ|X) = (1 + h(\frac{1}{3})) - 0 = \frac{1}{3} + \log 3 \approx 1.918$.

3.2 $f_{X_1X_2X_3}(0,0,0) = f_{X_1X_2X_3}(0,1,1) = f_{X_1X_2X_3}(1,0,1) = f_{X_1X_2X_3}(1,1,0) = \frac{1}{4}$,
så $f_{X_1}(0) = f_{X_1X_2X_3}(0,0,0) + f_{X_1X_2X_3}(0,1,1) = \frac{1}{2}$.
Similarly: $f_{X_1}(1) = f_{X_2}(0) = f_{X_2}(1) = f_{X_3}(0) = f_{X_3}(1) = \frac{1}{2}$, and $f_{X_1X_2}(00) = \cdots = \frac{1}{4}$.

a) $H(X_1) = H(\frac{1}{2}, \frac{1}{2}) = h(\frac{1}{2}) = 1$.

f) $H(X_3) = H(\frac{1}{2}, \frac{1}{2}) = 1$.

b) $H(X_1X_2) = H(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}) = \log 4 = 2$.

c) $H(X_2|X_1) = H(X_1X_2) - H(X_1) = 2 - 1 = 1$.

e) $H(X_3|X_1X_2) = 0$: if we know X_1 and X_2, we also know X_3.

d) $H(X_1X_2X_3) = H(X_1X_2) + H(X_3|X_1X_2) = 2 + 0 = 2$.

g) $H(X_1|X_3) = \frac{1}{2}H(X_1|X_3 = 0) + \frac{1}{2}H(X_1|X_3 = 1) = \frac{1}{2}H(\frac{1/4}{2/4}, \frac{1/4}{2/4}) + \frac{1}{2}H(\frac{1/4}{2/4}, \frac{1/4}{2/4}) = h(\frac{1}{2}) = 1$.
So $I(X_1;X_3) = H(X_1) - H(X_1|X_3) = 1 - 1 = 0$.

h) $I(X_1X_2;X_3) = H(X_3) - H(X_3|X_1X_2) = 1 - 0 = 1$.

3.3

X_1	X_2	X_3	$f_{X_1X_2X_3}$	f_{X_1}	$f_{X_2\|X_1}$
0	0	0	1/5	3/5	$\frac{2/5}{3/5} = 2/3$
0	0	1	1/5		
0	1	0	1/5		1/3
1	0	0	1/5	2/5	1/2
1	1	1	1/5		1/2

a) $H(X_1) = H(\frac{3}{5}, \frac{2}{5}) = h(\frac{2}{5}) = \log 5 - \frac{3}{5}\log 3 - \frac{2}{5} \approx 0.971$.

b) $H(X_2) = H(\frac{3}{5}, \frac{2}{5}) \approx 0.971$.

c) $H(X_3) = H(\frac{3}{5}, \frac{2}{5}) \approx 0.971$.

h) $H(X_2|X_1 = 0) = H(\frac{2}{3}, \frac{1}{3}) = h(\frac{1}{3}) = \log 3 - \frac{2}{3} \approx 0.918$.

i) $H(X_2|X_1 = 1) = H(\frac{1}{2}, \frac{1}{2}) = 1$.

d) $H(X_2|X_1) = \frac{3}{5}H(X_2|X_1 = 0) + \frac{2}{5}H(X_2|X_1 = 1) = \frac{3}{5}h(\frac{1}{3}) + \frac{2}{5} \cdot 1 = \frac{3}{5}\log 3 \approx 0.951$.

e) $H(X_1X_2) = H(X_1) + H(X_2|X_1) = h(\frac{2}{5}) + \frac{3}{5}\log 3 = \log 5 - \frac{2}{5} \approx 1.922$.

f) $H(X_3|X_1X_2) = \frac{2}{5}H(X_3|X_1X_2 = 00) = \frac{2}{5}h(\frac{1}{2}) = \frac{2}{5}$,
since if $X_1X_2 \neq (0,0)$, then X_3 is known, so $H(X_3|X_1X_2 \neq 00) = 0$.

g) $H(X_1X_2X_3) = H(X_1X_2) + H(X_3|X_1X_2) = (\log 5 - \frac{2}{5}) + \frac{2}{5} = \log 5 \approx 2.322$.

3.4 Let $Y =$ be the actual weather, $X =$ SMHI:s prediction and $Z =$ our prediction "always sunshine".

f_{XY}	$Y =$ rain	$Y =$ sunshine
$X =$ rain	1/4	1/2
$X =$ sunshine	0	1/4

f_{YZ}	$Y =$ rain	$Y =$ sunshine
$Z =$ rain	0	0
$Z =$ sunshine	1/4	3/4

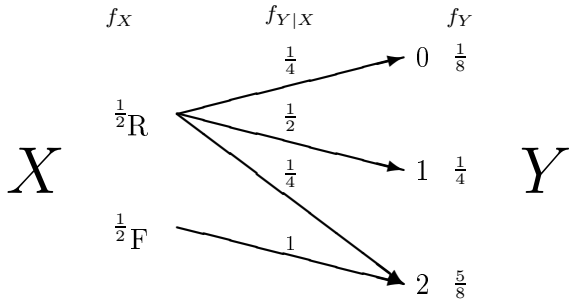
	f_X
$X = \text{rain}$	3/4
$X = \text{sunshine}$	1/4

f_Y	$Y = \text{rain}$	$Y = \text{sunshine}$
	1/4	3/4

$P(X = Y) = \frac{1}{2}$, and $P(Y = Z) = P(Y = \text{solsken}) = \frac{3}{4}$.
But $I(X;Y) = H(Y) - H(Y|X) = h(\frac{1}{4}) - [\frac{3}{4}h(\frac{1}{3}) + \frac{1}{4}h(0)] = h(\frac{1}{4}) - \frac{3}{4}h(\frac{1}{3}) = \frac{5}{2} - \frac{3}{2}\log 3 \approx 0.123$,
and $I(Y;Z) = H(Y) - H(Y|Z) = H(Y) - H(Y|Z = \text{sunshine}) = H(Y) - H(Y) = 0$.
If we know the stochastic property of the weather $P(\text{sunshine}) = \frac{3}{4}$, then we do not get any information from the prediction "always sunshine". But SMHI:s prediction gives some information: e.g., if the prediction is "sunshine", then we know it will not rain.

3.5 Using the same stochastic variables X and Y as in Exercise 3.4:
The uncertainty about the weather is $H(Y) = h(\frac{1}{2}) = 1$, and the remaining uncertainty about the weather *after* SMHI:s prediction is $H(Y|X) = [\frac{1}{2}h(0) + \frac{1}{2}h(0)] = 0$. Hence, we get the maximum information $I(X;Y) = H(Y) - H(Y|X) = 1 - 0 = 1$ about the weather Y from the prediction X.
Actually, we have no uncertainty about the weather if we know the prediction: It will rain if the prediction is "sunshine" and it will be sunshine if the prediction is "rain". The semantic meaning of "rain" and "sunshine" does not matter.

3.6 Let X be the choice of coin, so $f_X(\text{REAL}) = f_X(\text{FAKE}) = \frac{1}{2}$. Let Y be the number of "HEADS" in the tosses.



f_{XY}	$X = \text{REAL}$	$X = \text{FAKE}$
$Y = 0$	$\frac{1}{2} \cdot \frac{1}{4} = \frac{1}{8}$	0
$Y = 1$	$\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$	0
$Y = 2$	$\frac{1}{2} \cdot \frac{1}{4} = \frac{1}{8}$	$\frac{1}{2} \cdot 1 = \frac{1}{2}$

$I(X;Y) = H(Y) - H(Y|X) = H(\frac{1}{8}, \frac{1}{4}, \frac{5}{8}) - (\frac{1}{2}H(\frac{1}{4}, \frac{1}{2}, \frac{1}{4}) + \frac{1}{2}H(0,0,1))$
$= (\frac{1}{8}\log 8 + \frac{1}{4}\log 4 + \frac{5}{8}\log\frac{8}{5}) - \frac{1}{2}(\frac{1}{4}\log 4 + \frac{1}{2}\log 2 + \frac{1}{4}\log 4) - 0$
$= \frac{3}{8} + \frac{2}{4} + \frac{15}{8} - \frac{5}{8}\log 5 - \frac{2}{8} - \frac{1}{4} - \frac{2}{8} \qquad = 2 - \frac{5}{8}\log 5 \approx 0.549.$

3.7 For every non-trivial crypto system we have

$$H(\underline{M} \mid \underline{C}) \leq H(\underline{K} \mid \underline{C}) \leq H(\underline{K}).$$

So

$$\begin{aligned} I(\underline{M};\underline{C}) &= H(\underline{M}) - H(\underline{M} \mid \underline{C}) \geq \\ &\geq H(\underline{M}) - H(\underline{K}). \end{aligned}$$

We should choose a system with high uncertainty in the choice of key (large $H(\underline{K})$), e.g., many keys with same probability.

3.8 Assume that the key is given as $\underline{K} = K_0 K_1 \ldots K_{n-1}$.

$$\begin{aligned} H(\underline{K}) &= H(K_0) + H(K_1 \mid K_0) + \cdots + H(K_{n-1} \mid K_0 K_1 \ldots K_{n-2}) = \\ &= [K_i \text{ independent of } K_{i-1}] = \\ &= H(K_0) + H(K_1) + \cdots + H(K_{n-1}) = \\ &= [\text{"all have same probability"}] = \\ &= n \cdot H(K) = n \cdot \log(26) \end{aligned}$$

So the unicity distance is given by

$$N_0 = \frac{H(\underline{K})}{D} = \frac{n \cdot \log(26)}{3.2} = n \cdot 1.47$$

If two encryptions, with same period n, is done consecutively, the resulting key symbol at position i is given by

$$K_i = K_i^{(1)} + K_i^{(2)}.$$

Thus, we get a new Vigenère cipher, also with period n.

3.9 A Playfair cipher can be seen as a substitution cipher with an alphabet of 25 symbols. The uncertainty of the key is:

$$\begin{aligned} H(K) &= \log(25!) = \\ &= 22\log(2) + 10\log(3) + 6\log(5) + 3\log(7) + 2\log(11) + \log(13) + \log(17) + \log(19) + \log(23) \simeq \\ &\simeq 83.68 \end{aligned}$$

This gives the unicity distance

$$N_0 = \frac{83.68}{3.2} = 26.2.$$
