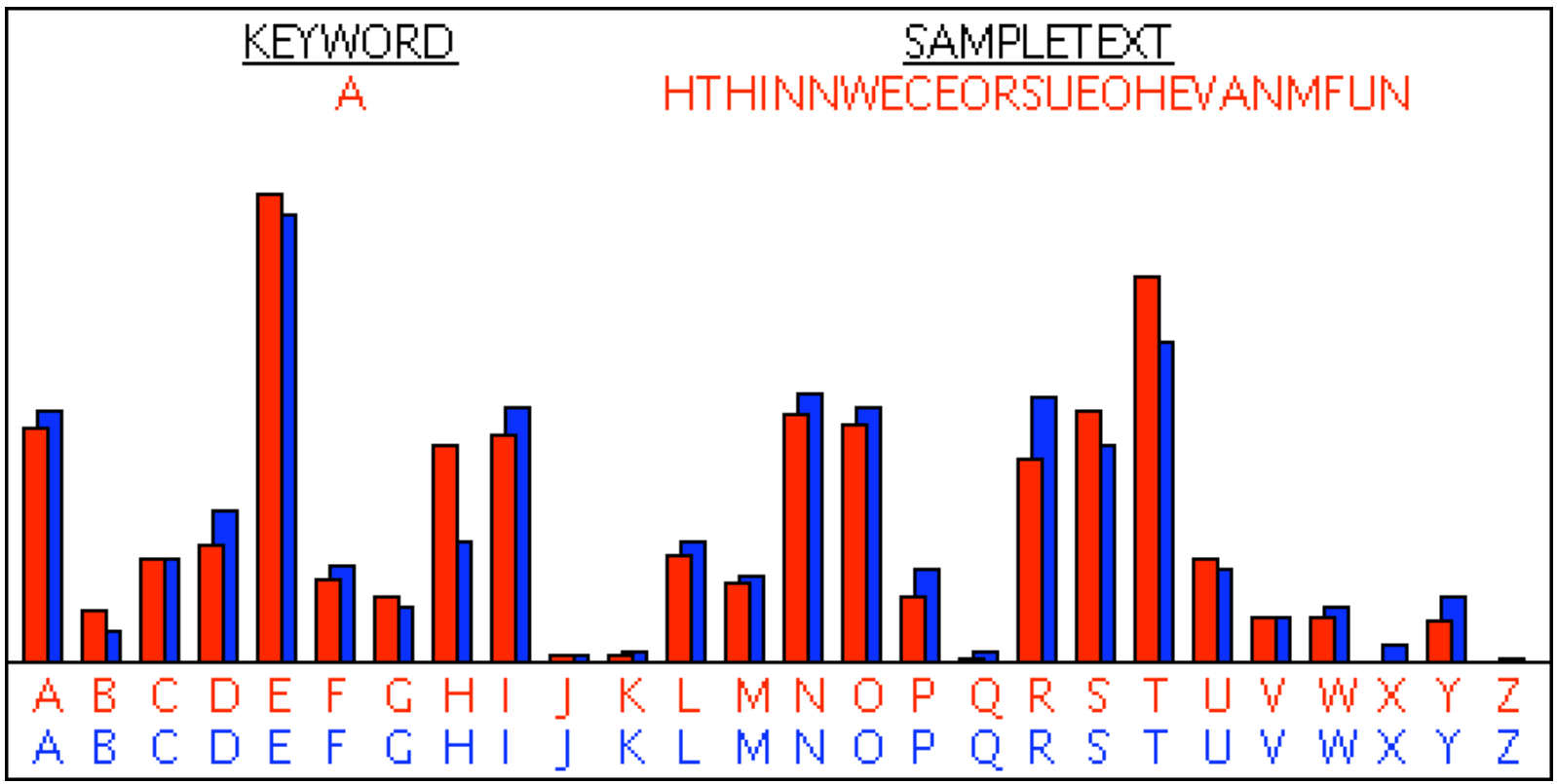
- Consider English text which is transformed by the rectangular transposition cipher.
- If we look at the single letter statistics they continue to look like English and hence they tell us nothing about how to recover the plaintext from the cyphertext.



Recall how we encrypt cyphertext using the rectangular transposition cipher.

$\sigma(1)$	$\sigma(2)$	$\sigma(3)$	$\cdots$	$\sigma(p)$
a_1	a_2	a_3	$\cdots$	a_p
a_{p+1}	a_{p+2}	a_{p+3}	$\cdots$	a_{2p}
$\vdots$				$\vdots$
a_{kp+1}	a_{kp+2}	a_{kp+3}	$\cdots$	$a_{(k+1)p}$

plaintext:

$$a_1 a_2 \cdots a_p a_{p+1} a_{p+2} \cdots a_{2p} \cdots$$

cyphertext:

$$a_{\sigma^{-1}(1)} a_{\sigma^{-1}(2)} \cdots a_{\sigma^{-1}(p)} a_{p+\sigma^{-1}(1)} a_{p+\sigma^{-1}(2)} \cdots a_{p+\sigma^{-1}(p)} \cdots$$

Recall how we encrypt cyphertext using the rectangular transposition cipher.

$\sigma(1)$	$\sigma(2)$	$\sigma(3)$	$\cdots$	$\sigma(p)$
a_1	a_2	a_3	$\cdots$	a_p
a_{p+1}	a_{p+2}	a_{p+3}	$\cdots$	a_{2p}
$\vdots$				$\vdots$
a_{kp+1}	a_{kp+2}	a_{kp+3}	$\cdots$	$a_{(k+1)p}$

plaintext:

$$a_1 a_2 \cdots a_p a_{p+1} a_{p+2} \cdots a_{2p} \cdots$$

cyphertext:

$$a_{\sigma^{-1}(1)} a_{\sigma^{-1}(2)} \cdots a_{\sigma^{-1}(p)} a_{p+\sigma^{-1}(1)} a_{p+\sigma^{-1}(2)} \cdots a_{p+\sigma^{-1}(p)} \cdots$$

Yes, we're using the *other* version of rectangular transposition where we read the rows and not the columns.

Guess at the period p of the cyphertext.
Let a and b represent letters and for $1 \leq i, j \leq p$

$N_{a,b}^{(i,j)}$ = the number of pairs of letters equal to a, b where a is in the i^{th} position in the blocks of p and b is in the j^{th} position.
Let N = the number of letters in the cyphertext divided by p
Let $p_{a,b}$ = the probability that ab occurs in English.

- If the letters in the j^{th} position in the cyphertext are supposed to follow the letters in the i^{th} position, then the transition is 'good' and we should expect to see $N_{a,b}^{(i,j)}$ to be roughly equal to $N * p_{a,b}$.
- If the letters in the j^{th} position in the cyphertext are not supoosed to follow the letters in the i^{th} position, then the transition is 'not good' and and we should expect to see $N_{a,b}^{(i,j)} = N * q_{a,b}$ for some other probabilities $q_{a,b}$.

Now calculate

$$\sum_{a,b=A}^{Z} p_{a,b} \log N_{a,b}^{(i,j)}$$

- If the $i \longrightarrow j$ transition is 'good' then $N_{a,b}^{(i,j)} \approx N * p_{a,b}$ and

$$\sum_{a,b=A}^{Z} p_{a,b} \log N_{a,b}^{(i,j)} \approx \log N + \sum_{a,b=A}^{Z} p_{a,b} \log p_{a,b}$$

- If the $i \longrightarrow j$ transition is 'not good' then $N_{a,b}^{(i,j)} \approx N * q_{a,b}$ and

$$\sum_{a,b=A}^{Z} p_{a,b} \log N_{a,b}^{(i,j)} \approx \log N + \sum_{a,b=A}^{Z} p_{a,b} \log q_{a,b}$$

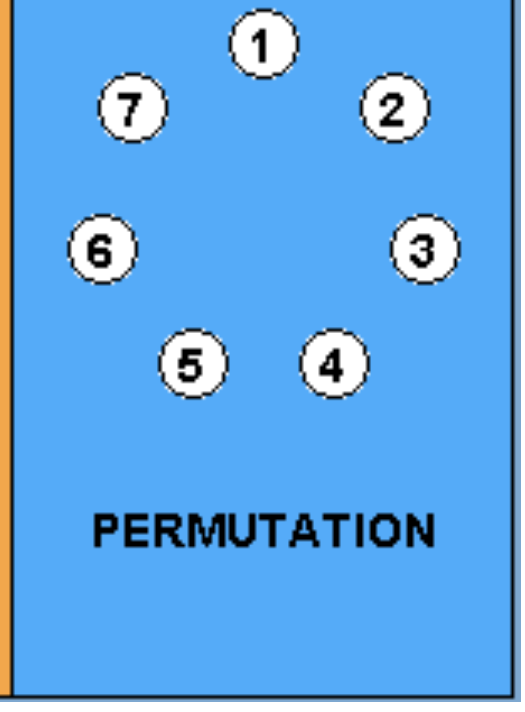
- Recall that we derived the inequality

$$\sum_{i} p_i \log q_i \leq \sum_{i} p_i \log p_i.$$

Example of table of $\sum_{a,b=A}^{Z} p_{a,b} \log N_{a,b}^{(i,j)}$ with correct period

We should see high values in each row and column except one row (the last position of the permutation) and one column (the first position of the permutation).

0	26	31	34	26	20	36
18	0	53	32	24	32	27
39	26	0	26	24	29	18
27	19	33	0	26	28	22
24	39	29	29	0	26	21
21	28	28	44	27	0	23
29	26	28	23	25	43	0



Example of table of $\sum_{a,b=A}^{Z} p_{a,b} \log N_{a,b}^{(i,j)}$ with incorrect period

We should see high and low values evenly distributed in the table.

0	18	17	18	23	23	23
17	0	14	19	21	25	20
25	16	0	20	19	20	20
24	32	18	0	25	21	20
20	20	23	19	0	28	24
22	23	20	19	21	0	24
25	23	14	21	24	22	0