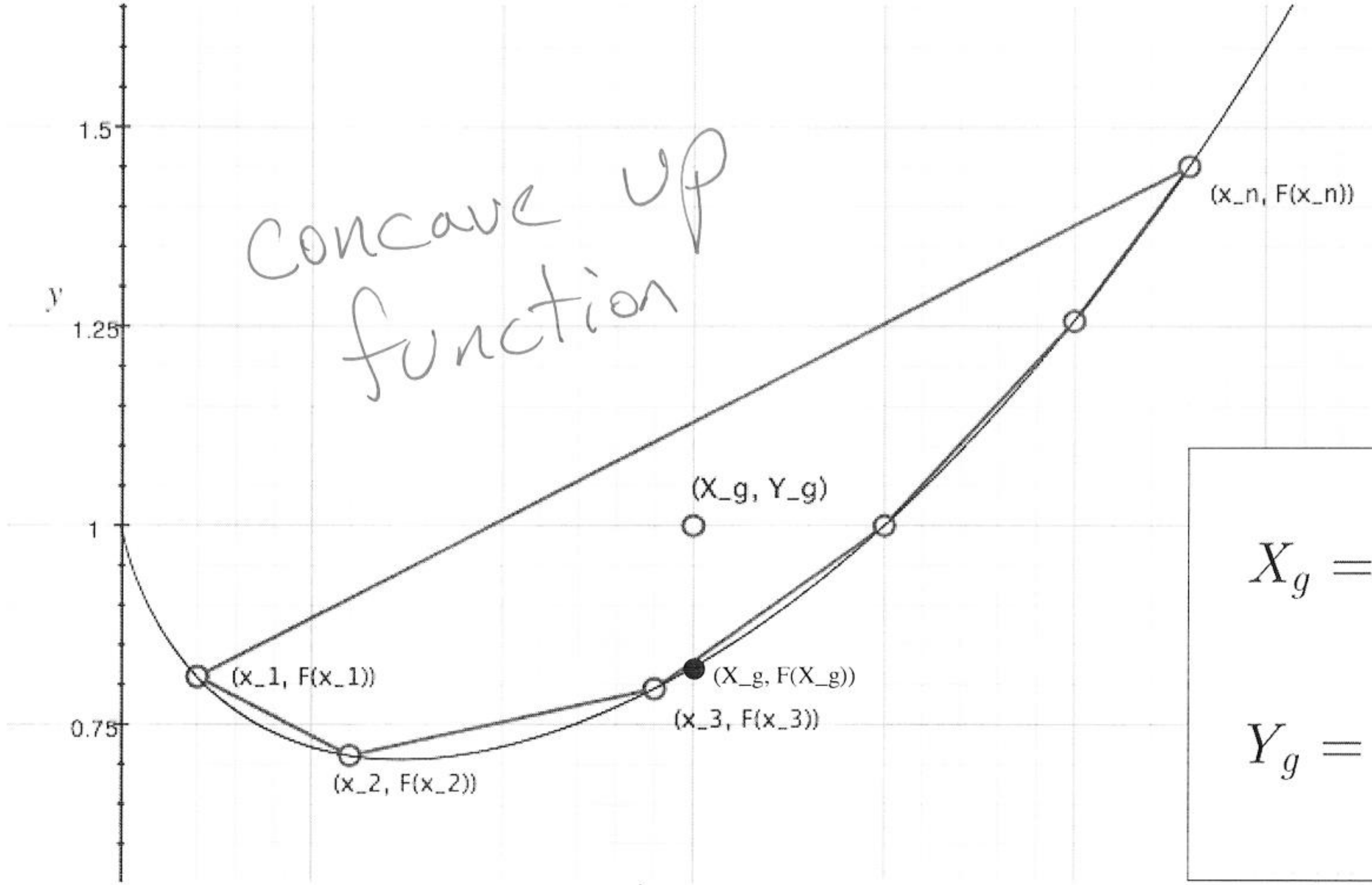


$m_i \geq 0$

$$\sum_{i=1}^{n} m_i = 1$$

$$X_g = \sum_{i=1}^{n} m_i x_i$$

$$Y_g = \sum_{i=1}^{n} m_i F(x_i)$$

$$F\left(\overset{\overset{F(X_g)}{\parallel}}{\sum_{i=1}^{n} m_i x_i}\right) = F(X_g) \leq Y_g = \sum_{i=1}^{n} m_i F(x_i)$$

$$\log(ab) = \log a + \log b$$

$$\log(a/b) = \log a - \log b$$

$$a\log(b) = \log(b^{a})$$

$$\frac{d}{dx}(\log_e x) = \frac{1}{x}$$

$$F'(x) = \log x + x \cdot \frac{1}{x}$$
$$= \log x + 1$$
$$F''(x) = \frac{1}{x}$$

$$\boxed{F(x) = x \log x}$$

$$\boxed{F\left(\sum_{i=1}^{n} m_i x_i\right) \leq \sum_{i=1}^{n} m_i F(x_i)}$$

$$\boxed{x_i = p_i/q_i} \qquad \boxed{m_i = q_i}$$

$$\sum_{i=1}^{n} m_i x_i = \sum_{i=1}^{n} q_i p_i/q_i = \sum_{i=1}^{n} p_i = 1$$

A simple test for monoalphabetic substitution

English:	MISSISSIPPI
Monoalphabetic:	RDFFDFFDOOD
Vigenere :	PQJLLAJBSXZ

In English or monoalphabetic encrypted text we observe:

$$p_{AA} + p_{BB} + p_{CC} + \cdots + p_{ZZ} \approx .027$$

While in polyalphabetic cyphertext we should observe:

$$P(\alpha\alpha \text{ occurrs in random cyphertext }) = \frac{1}{26} \approx .038$$

test cyphertext $\frac{\#\text{ of equal adjacent pairs}}{\text{total }\#\text{ of adjacent pairs}} = \frac{}{N-1}$

We should note (of course) that this only works for reasonably large amounts of text.

XYZABC

If there are N letters in plaintext there are N-1 adjacent pairs

A simple test for monoalphabetic substitution

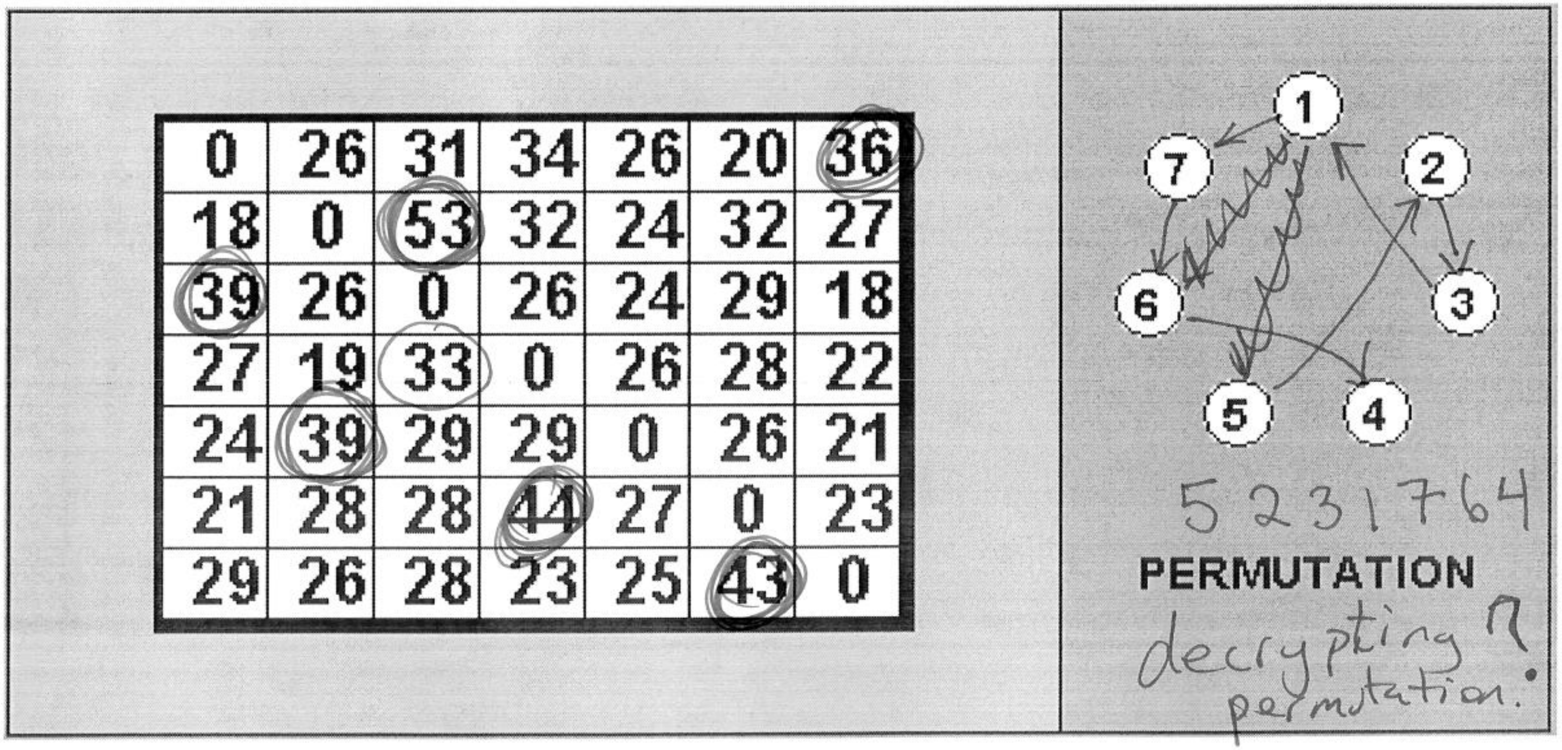
English:	`MISSISSIPPI`
Monoalphabetic:	`RDFFDFFDOOD`
Vigenere :	`PQJLLAJBSXZ`

In English or monoalphabetic encrypted text we observe:

$$\underbrace{p_{AA}}_{\text{probability that AA occurs next to each other in plaintext}} + p_{BB} + p_{CC} + \cdots + p_{ZZ} \approx .027$$

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

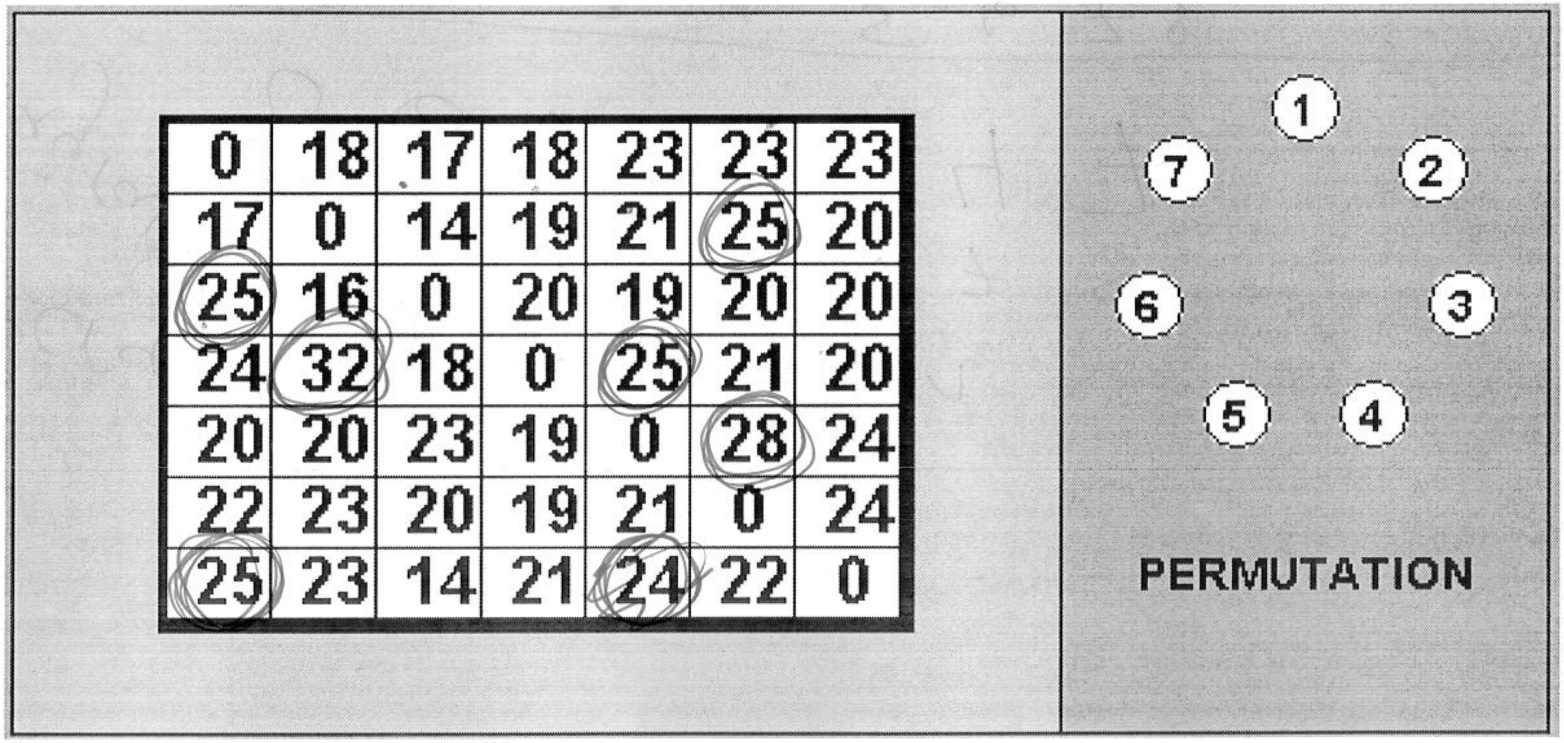
5 2 3 1 7 6 4

PERMUTATION

decrypting ?
permutation.

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

decrypting permutation

diagram	8	6	5	3	1	2	4	7
	1	2	3	4	5	6	7	8
encrypting perm	5	6	4	7	3	2	8	1