Tutorial 3

Problem 1 / a) The autokey cryptosystem:

$$c_i = \begin{cases} m_i + k_i \mod 26 & 0 \le i \le n-1 \\ m_i + c_{i-n} \mod 26 & n \le i \le l-1 \end{cases}$$

Using a ciphertext only attack, we can compute the msg as follows

$c_n = m_n + c_0 \mod 26 \iff m_n = c_n - c_0 \mod 26$

$c_{n+1} = m_{n+1} + c_1 \mod 26 \iff m_{n+1} = c_{n+1} - c_1 \mod 26$

$\Rightarrow m_{n+j} = c_{n+j} - c_j \mod 26 \quad \forall\ 0 \le j \le l-1-n$

$\Rightarrow m_j = c_j - c_{j-n} \mod 26 \quad \forall\ n \le j \le l-1$

We try $n = 1, 2, \ldots$ until the deciphered text sounds reasonable

b) $n = 1$

c_j	D	L	G	V	T	Y	...
c_{j-1}		D	L	G	V	T	...
m_j		I	V	P			

$n = 2$

c_j	D	L	G	V	T	Y
c_{j-2}			D	L	G	V
m_j			D	K	N	

$n = 3$

c_j	D	L	G	V	T	Y	O	A	C	O	U	V	C	E	Z	A
c_{j-3}	K	E	Y	D	L	G	V	T	Y	O	A	C	O	U	Y	C
m_j	T	H	I	S	I	S	T	H	E	A	U	T	O	K	E	Y

The key would be 'THI' - 'DLG' = 'KEY'

c) Consider:

$$\hat{c}_i = \begin{cases} m_i + k_i \mod 26 & 0 \le i \le n-1 \\ m_i + m_{i-n} \mod 26 & n \le i \le l-1 \end{cases}$$

Now we assume to know the keylength n, and we know the construction of the cryptogram. We do a frequency analysis on

$$\hat{c}_i = m_i + m_{i-n} \qquad n \le i \le l-1$$

With a Friedmann attack we determine the most frequent $\hat{c}_i$. This is 'i' and the most likely combination to get it is 'e' + 'e'

Assume $\hat{c}_k = 'i'$, $k \ge n$

$$m_{k-(j+1)n} = \hat{c}_{k-jn} - m_{k-jn} \mod 26 \quad \forall j \in \mathbb{N} \text{ with } k-jn \ge n.$$

$$m_{k+jn} = \hat{c}_{k+jn} - m_{k+(j-1)n} \mod 26 \quad \forall j \in \mathbb{N} \text{ with } k+jn < l$$

d) In our case there are two positions with 'i'.

Q	E	X	Y	I	R	V	E	S	I	U	X	X	K	Q	V	F	L	H	K	G
T	E		E	R		B		T		E			M		T	O		S		
	H		R	A		E		E		T		R		E	H	D				

The key is 'QE' - 'TH' = '++'

Problem 2 | Follow Kasiski-Babbage method

$$\Rightarrow k \approx \frac{0.028433\, n}{(n-1)I_c - 0.0385 \cdot n + 0.066895}$$

$$E(I_c) \approx \frac{1}{n(n-1)} \sum_{\ell=0}^{m-1} n_\ell (n_\ell - 1) = I_c$$

In our case $k = 5$ (from hint)

Take most frequent letters from each block

Block			
1	'T'	- 'E'	= 'P'
2	'P'	- 'E'	= 'L'
3	'Y'	- 'E'	= 'V'
4	'X'	- 'E'	= 'T'
5	'S'	- 'E'	= 'O'

The key is most likely PLUTO