Network and Information Security
Lecture 10

B.Tech. Computer Engineering
Sem. VI.

Prof. Mrudang T. Mehta
Associate Professor
Computer Engineering Department
Faculty of Technology,
Dharmsinh Desai University, Nadiad

Cryptanalysis of Vigenere Cipher (Continue...)

1. For two strings x and y ciphered using keys k_i and k_j the value of $MI_c(x, y)$ depends on the difference $k_i - k_j$ (mod 26).
2. A relative shift of s yields the same value as 26 –s.

When $k_i - k_j = 0$, the value of MI_c, is maximum and is equal to 0.065. However, for other values, the estimate is comparatively less and ranges from 0.032 to 0.045 on an average.

- So in order to find the actual key, we divide the given string of encrypted characters into m rows.
- Each row is a shift cipher, which has been shifted by a key, k_i.
- Thus for each row we find the Mutual Index of Coincidence with respect to an unencrypted english text.
- We compute the MI values by varying the keys, k_i from 0 to 25.
- The values for which the MI values become close to 0.065 will indicate the correct key, k_j .
- This process is repeated for the m rows to obtain the entire key.

Example

- Let us assume we have intercepted the following cipher text:

  LIOMWGFEGGDVWGHHCQUCRHRWAGWIOWQLKGZETKKMEVLWPCZVGTHVTS
  GXQOVGCSVETQLTJSUMY.WVEUVLXEWSLGFZMVVWLGYHCUSWXQHKVGSHEEV
  FLCFDGVSUMPHKIRZDMPHHBVWVWJWIXWIXGFWLTSHGJOUEEHHVUCFVGOW
  ICQLTJSUXGLW.

- The Kasiski test for repetition of three-character segments yields the results shown in Table

String	First Index	Second Index	Difference
QLT	65	165	100
LTJ	66	166	100
TJS	67	167	100
JSU	68	168	100
SUM	69	117	48
VWV	72	132	60

- The greatest common divisor of differences is 4, which means that the key length is multiple of 4.
- We try confirm this guess by the Index of Coincidence test.
- We divide the ciphertext into 4 rows.
- We also mention the corresponding index of coincidence values.
- The high values of the IC confirms the key length reported by the kasiski test.

1st String IC=0.067677	LWGWCRAOKTEPGTQCTJVUEGVGUQGECVPRPVJGTJEUGCJG
2nd String IC=0.074747	IGGGQHGWGKVCTSOSQSWVWFVYSHSVFSHZHWWFSOHCOQSL
3rd String IC=0.070707	OFDHURWQZKLZHGVVLUVLSZWHWKHFDUKDHVIWHUHFWLUW
4th string IC=0.076768	MEVHCWILEMWVVXGETMEXLMLCXVELGMIMBWXLGEVVITX

First line is made up of characters 1,5,9,....,Second line is 2,6,10,....and so on.

- Thus we perform the Mutual index of coincidence to obtain the actual key value. Running the test, we obtain that the key value is CODE and the corresponding plain text is:

- Julius Caesar used a cryptosystem in his wars, which is now referred to as Caesar cipher. It is an additive cipher with the key set to three. Each character in the plain text is shifted three characters to create ciphertext.