Fundamentals of Information & Network Security
ECE 471/571

Lecture #7: Cryptanalysis (continued)

Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Attack models

Ciphertext-only attack: Eve only observes the ciphertext y

Known-plaintext attack: Eve knows some plaintext x and its corresponding ciphertext y

Chosen-plaintext attack: Eve has temporary access to an encryption box.
It can feed any chosen plaintext x and obtain the ciphertext y

Chosen-ciphertext attack: Eve has temporary access to a decryption box.
It can feed any chosen ciphertext y and obtain the plaintext x

Example:

Perform each type of attack on a shift cipher. Comment on the complexity of performing each attack

Plaintext x: shift   ciphertext y: vkliw

Question: for brute-force attack, on average, how many keys must be tried to achieve success?

Cryptanalysis of the Affine Cipher

- Ciphertext only attack

Example:
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEV
LRHHR

- Known plaintext attack

Cryptanalysis of the Affine Cipher

Plaintext:

algorithms are quite general definitions of arithmetic processes

Cryptanalysis of the Hill Cipher

- Difficult to break with ciphertext-only attack

- Known-plaintext attack
  – Given some (plaintext, ciphertext) pairs, create a matrix equation $Y = XK$ and solve for K by inverting matrix X.
  – Example: $m = 2$ and the plaintext is friday yielding a ciphertext PQCFKU.

Cryptanalysis of the Vignere Cipher

- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack
- Ciphertext only attack
  - Why hard?

Frequency Distributions of Different Ciphers

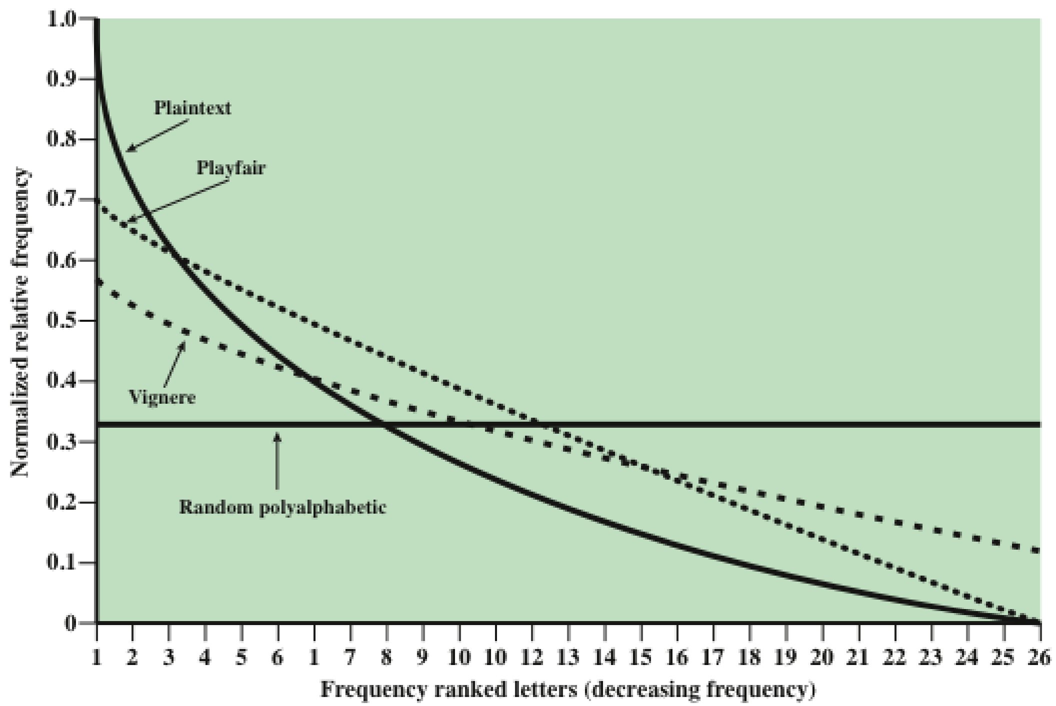


Figure 3.6 Relative Frequency of Occurrence of Letters

Cryptanalysis of Vignere Cipher

- Observation: consists of multiple monoalphabetic ciphers

- Method

1. Determine the key length.
   - *Index of coincidence, Kasiski test*
2. Break the ciphertext into sub-pieces encrypted with the same key letter.
3. Solve each piece as a monoalphabetic cipher.

Finding Key Vector Length

- Index of coincidence
  - Probability that two randomly chosen elements of a string are identical.
  - If we have the correct key vector length m, IC is about 0.065. Random ciphertext: 0.038.

$$I_c(\underline{\mathrm{x}}) = \sum_{i=0}^{25} \frac{\binom{f_i}{2}}{\binom{n}{2}}$$

- Kasiski Test
  - Distance of pairs of identical segments of ciphertext of length at least three.
  - Compute the gcd of those distances, and the most common gcd is the key length

Finding Key Vector Length

- Example

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBWRVXUOAKXAO
SXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAKLXFPSKAUTEMNDCMGTSX
MXBTUIADNGMGPSRELXNJELXVRVPRTULHDNQWTWDTYGBPHXTFALJHA
SVBFXNGLLCHRZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBIPEEWEVKAKO
EWADREMXMTBHHCHRTKDNVRZCHRCLQOHPWQAIIWXNRMGWOIIFKEE

- CHR cipher appears at 1, 166, 236, 276, 286 start locations. So the distances from 1st occurence to other four occurences are 165, 235, 275, 285 respectively.
- According to the Kasiski Test the gcd of these distances being 5, is the most likely length of the key vector.

Finding the Key

- For each cipher piece, check the "shifted IC" (for all 0<g<26):

$$M_g = \sum_{i=0}^{25} \frac{p_i f_{i+g}}{n'} \stackrel{?}{\approx} \sum_{i=1}^{25} p_i^2 = 0.065$$

j	M_g								
	.035	.031	.036	.037	.035	.039	.028	.028	.048
1	**.061**	.039	.032	.040	.038	.038	.045	.036	.030
	.042	.043	.036	.033	.049	.043	.042	.036	
	.069	.044	.032	.035	.044	.034	.036	.033	.029
2	.031	.042	.045	.040	.045	.046	.042	.037	.032
	.034	.037	.032	.034	.043	.032	.026	.047	
	.048	.029	.042	.043	.044	.034	.038	.035	.032
3	.049	.035	.031	.035	**.066**	.035	.038	.036	.045
	.027	.035	.034	.034	.036	.035	.046	.040	
	.045	.032	.033	.038	**.060**	.034	.034	.034	.050
4	.033	.033	.043	.040	.033	.029	.036	.040	.044
	.037	.050	.034	.034	.039	.044	.038	.035	
	.034	.031	.035	.044	.047	.037	.043	.038	.042
5	.037	.033	.032	.036	.037	.036	.045	.032	.029
	.044	**.072**	.037	.027	.031	.048	.036	.037	

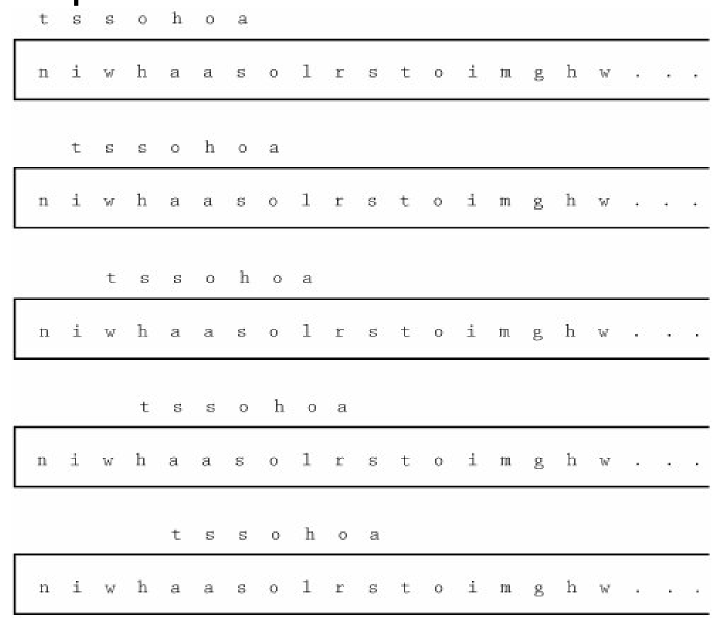
Table 1. $Q_j = \sum_{i=0}^{25} \frac{p_i f_{i+g}}{n'}$.

K = (9, 0, 13, 4, 19)
or, JANET.

Cryptanalysis of Columnar Transposition

- Brute force
- Diagram analysis
  - Moving comparisons

Ciphertext:
tssohoaniwhaasolrstoimghw
utpirseeoamrookistwcnasns



This is a message to show how
a columnar transposition works.

How to Determine the Cipher Type?

- Frequency analysis
- Index of coincidence
- …

Reading

- Textbook Appendix F (measures of security and secrecy)
  - Can be found online