Vigenère Ciphers

Caesar Ciphers (and Affine transformation ciphers) are too weak and suffer from frequency analysis attacks (or more simply brute force attacks).

For Example: Encrypt MILLENNIUM using the keyword YTWOK

M	I	L	L	E	N	N	I	U	M	S		Y	T	W	O	K
12	8	11	11	4	13	13	8	20	12	18		24	19	22	14	10
+ 24	19	22	14	10	24	19	22	14	10		$\equiv$ mod 26.					
10	1	7	25	14	11	6	4	8	22	16						
K	B	H	Z	O	L	G	E	I	W	Q						

Idea: Use each letter in the keyword to encrypt the plaintext. Also combine with a full affine transformation cipher. For example

A	P	P	L	E
0	15	15	11	4
k_1	k_2	k_1	k_2	k_1
1	22	20	10	13
B	W	U	K	N

Keys: $[\underset{a_1\ b_1}{(3,1)}, \underset{a_2\ b_2}{(3,3)}]$ (k_1, k_2) $\quad C \equiv a_i P + b_i \bmod 26$

$C \equiv 3P+1 \bmod 26$ $\quad C \equiv 3P+3 \bmod 26$

$C \equiv 3(0)+1 \equiv 1 \bmod 26$ $\quad C \equiv 3(15)+3 \equiv 22 \bmod 26$

$C \equiv 3(15)+1 \equiv 20 \bmod 26$. $\quad C \equiv 3(11)+3 \equiv 16 \bmod 26$

$C \equiv 3(4)+1 \equiv 13 \bmod 26$.

We will call the second encryption an Affine Vigenère Cipher.

Example: Encrypt the message

PINOCCHIO IS A BOY

using a Vigenere cipher with the key word TOY. For reference, you may use

	A	B	C	D	E	F	G	H	I	J	K	L	M
P	00	01	02	03	04	05	06	07	08	09	10	11	12
C	19												
	T												
C	14												
	O												
C	24												
	Y												
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	13	14	15	16	17	18	19	20	21	22	23	24	25
C													
C													
C													

If you'll have an, you can encrypt/decrypt just as (potentially).

T O Y
19 14 24

P I N O C C H I O I S A B O Y
15 8 13 14 2 2 7 8 14 8 18 0 1 14 24
+ 19 14 24 19 14 24 19 14 24 19 14 24 19 14 24 mod 26
8 22 11 7 16 0 0 22 12 1 6 24 20 2 22
I W L H Q A A W M B G Y U C W

Now decipher the message

ZSNIS RMCGL OKTB

using the same encryption scheme above

Z S N I S R M C G L O K T B
25 18 13 8 18 17 12 2 6 11 14 10 19 1
- 19 14 24 19 14 24 19 14 24 19 14 24 19 14 mod 26.
6 4 15 15 4 19 19 14 8 18 0 12 0 13
G E P P E T T O I S A M A N

Frequency Analysis

What is the most common English letter?

E T A O I N S ... see wikipedia

~~13%~~ 12.7% 9.1% 8.2% 7.5%

So in an encrypted text, if M is the most likely letter, it is likely that E ↦ M.

This would help with breaking Caesar and Affine Transformation ciphers.

This alone will not help w. the Vigenère cipher. First attack ~1863 named after Friedrich Kasiski.

Kasiski's Test: Look for ~~repeat~~ repeated strings of length 3 or more

Once you have a guess of the key length, attempt to decipher OR verify your guess using the index of Coincidence (see Friday's lecture).

ENCIPHERING MESSAGES.

Consequently, we made the correct guess. If we had tried this transformation, and instead of plaintext, it produced garbled text, we would have tried another likely transformation based on the frequency count of letters in the ciphertext. ◀

Example 8.5. Suppose we know that an affine transformation of the form $C \equiv aP + b \pmod{26}$, $0 \leq C \leq 25$, has been used for encryption. For instance, suppose that we wish to cryptanalyze the encrypted message

USLEL	JUTCC	YRTPS	URKLT	YGGFV
ELYUS	LRYXD	JURTU	ULVCU	URJRK
QLLQL	YXSRV	LBRYZ	CYREK	LVEXB
RYZDG	HRGUS	LJLLM	LYPDJ	LJTJU
FALGU	PTGVT	JULYU	SLDAL	TJRWU
SLJFE	OLPU.			

The first thing to do is to count the occurrences of each letter; this count is displayed in Table 8.7.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number of Occurrences	2	2	4	4	5	3	6	1	0	10	3	22	1	0	1	4	2	12	7	8	16	5	1	3	10	2

Table 8.7 *The number of occurrences of letters in a ciphertext.*

With this information, we guess that

Example 8.8. Suppose that the ciphertext produced by encrypting plaintext using a Vigenère cipher is

QWHID	DNZEM	WTLMT	BKTIT	EMWLZ
WVCVE	HLTBS	TUDLG	WNUJE	WJEUL
EXWQO	SLNZA	NLHYQ	ALWEH	VOQWD
VQTBW	ILURY	STIJW	CLHWW	RNSIH
MNUDI	YFAVD	ELAGB	LSNZA	NSMIF
GNZEM	WALWL	CXEFA	BYJTS	SNXLH
YHULK	UCLOZ	ZAJHI	HWSM	

We describe the steps we use to break this message. We first use the Kasiski test, looking for repeated triples of letters in the ciphertext. We list our finding in a table.

Triple	Starting positions	Differences in starting positions
EMW	9, 21, 129	12, 108, 120
ZEM	8, 128	120
ZAN	59, 119	60
NZE	7, 127	120
NZA	58, 118	60
[illegible]	62, 149	87