VIGENERE CIPHER

- In a Caesar cipher, each letter of the alphabet is shifted along some number of places; for example, in a Caesar cipher of shift 3, A would become D, B would become E and so on.
- The Vigenère cipher consists of several Caesar ciphers in sequence with different shift values.
- To encrypt, a table of alphabets can be used, termed a tabula recta, *Vigenère square*, or *Vigenère table*
- It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers.

VIGENERE CIPHER (Conti…)

- Plain text: ATTACKATDAWN
- Key: LEMON

A	T	T	A	C	K	A	T	D	A	W	N
L	E	M	O	N	L	E	M	O	N	L	E

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

- Cipher text :LXFOPVEFRNHR

VIGENERE CIPHER (Conti…)

- Plaintext: information security
- Key: confidential
- Encryption: KBSTZPEGBWNDGQHWQWC

- Plaintext: crypto is for cryptography
- Key: abcdef
- Encryption: CSASXTITHRVHRZRWSLRBRKC

VIGENERE CIPHER (Conti…)

- Vigenère can also be viewed algebraically. If the letters A–Z are taken to be the numbers 0–25, and addition is performed modulo 26, then Vigenère encryption can be written,

$$C_i \equiv (P_i + K_i) \pmod{26}$$

- Decryption

$$P_i \equiv (C_i - K_i) \pmod{26}$$

VERNAM CIPHER

- Gilbert vernam in 1918 devised a system that works on binary data rather than letters.

Encryption : $c_i = m_i \oplus k_i \qquad i = 1,2,3,...$

m_i : plain-text bits.

k_i : key (key-stream) bits

c_i : cipher-text bits.

Decryption : $m_i = c_i \oplus k_i \qquad i = 1,2,3,...$

- Vernam proposed the use of running tape that eventually repeated the key, so that the system can work with a very but repeating keys

ONE-TIME PAD

- Major joseph mauborgne-an army signal corp. officer, invented it by proposing improvement in vernam cipher.
- A one-time pad (OTP) is a large no repeating set of truly random key letters, written on sheet of paper, and glued together in a pad.
- The sender uses each key letter on the pad to encrypt exactly one plain text character.
- The sender encrypts the message and then destroys the used pages of the pad.
- The receiver has an identical pad and uses each letter on the pad, in turn, to decrypt each letter of cipher text.
- The receiver destroys the same used pages of the pad after decrypting the message.
- It produces random output that bears no statistical relationship to the plaintext so there is no way to break the code.