

A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Semester: VI Subject: CSS Academic Year: 20 28-202-4
Autokey Copher:
The key in the autokey apher is a stream of eubheys, each of which is used to encrypt the plaintext character it
each of which is used to encrypt the plaintext character it
corresponde lo
* The fact subkey is a secretly agreed upon value
* The first subkey is a secretly agreed-upon value among the communicating parties. The value of the first
plaintent character is the second subby
alaintent character is the second subby. The value of the second plaintent character is the
third subkey, and so on.
third subkey, and so on: # Given plaintent P=P1P2P2 and key K= (K1, P1, P2)
Encuption: C: = (P:+K:) mod 26
Decryption: Pi = (Ci-Ki) mod 26.
Examples:
Enought the message "ATTACK IS TODAY using authory april.
with key=12. Ignore the space between words.
Examples:- Encrypt the message "ATTACK IS TODAY" using autokey cipher with key=12. Ignore the space between words.
Encryption: Ci = (P,+K;) mod 26.
U.

Plain Text	A	T	T	A	(K	1	S	T	D	D	Α	Y
Ps Values	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream	12	00	19	19	00	02	10	08	18	19	14	03	00
Cé value	12	19	12	19	02	12	18	00	11	07	17	03	24
CopherTent	M	T	M	T	C	M	S	A	L	H	R	D	Y

The result is "MTMTCMSALHRDY".

Subject Incharge: Prof. Sarala Mary Page No. 2

Department of CSE-Data Science | APSIT

