HASHIM Abdulhadi
16/ENG02/062

Autokey Ciphers :

An Autokey Cipher is a substitution cipher that uses the plaintext itself as a key, along with a keyword placed at the beginning of the plaintext. Then, a Vigenère table is used to encipher the keyed plaintext.

Example

Plaintext: Whoever has made a voyage up the Hudson must remember the Kaatskill mountains.

Key: WINKLE

Encipher step:

Keyed Text: WINKLEWHOEVERHASMADEAVOYAGEUPTHEHUDSONMUSTREMEMBERTHEKAATSKILLMOU

Plain Text: whoeverhasmadeavoyageupthehudsonmustremembertheKaatskillmountains

Ciphertext: (coming soon)

Vulnerabilities of Autokey Cipher

Since the key is in English, using short English words along the length of the cipher text could reveal likely English results. This can be used to guess the length of the keyword and ultimately reveal it.

How to Crack an Autokey Cipher

Use a common short word and try it out as the key text. Look for likely English results in the resulting plaintext. Use this to guess at the length of the keyword. Shift the likely results back to find the keyword at the beginning of the shifted plaintext.

Computer Crimes:

Defined broadly, the term 'computer crime' could reasonably include a wide variety of criminal offences and unlawful activities related to or having connection to computers. The potential scope is even larger when using the frequent companion or substitute term 'computer-related crime'.

Computer crimes can be classified essentially under two headings; where computer is either (a) a tool, or (b) a target, to perform an unlawful act.

2 The computer is a tool for an unlawful act where the offence reflects a modification of a conventional crime by making use of information technology and modern communication tools. There are certain crimes where the computer itself is the target, that is, to say such crimes which have evolved due to the advancement in information technology itself.

Of course, there might be instances where the computer is a tool as well as the target of a crime. This kind of activity usually involves sophisticated crimes usually out of the purview of conventional criminal law.

There is a third category as well, where computers are considered as incidental to a crime.

3 The use of a computer is not necessary but are used to make the offender more efficient in the commission of the crime. This includes use of computers in bookmaking or drug-dealing. There is another way in which crime on the Internet can be looked into. The Internet is a network of computers that communicate with each other. Information generated within a computer and available to be shared with other computers connected to a network is what the Internet is about. Some computers provide information, some seek information, some provide the mechanism for smooth exchanges and some route the flow of information.

Thus criminal conduct within this definition of Internet can arise whenever there is: A conduct in a manner so as to adversely affect a computer (hacking, cracking, illegal downloading of information stored on a computer, virus or worm attack, etc.). Conduct so as to affect a person - maybe an industry, government or a private individual (e.g., child pornography, spamming, defamation, threats, posting a copyright material etc.). The difference between crime committed through computers vis-a-vis those committed with the help of any other modern technology like the telephone is crucial. While crimes are rarely directed against a telephone as an instrument, computers often become the victims of attack

.4 Nature of crime on the computer is challenging and requires new definitions and understanding and a restatement of accepted norms of criminal conduct and punishment because of several reasons. Computers apart from being costly equipment is also the repository of immense amount of data. This data can sometime contain valuable scientific inputs, purely personal matter, study.