Tiny Encryption Algorithm

Tiny encryption algorithm is one of the fast, simple and efficient cryptographic algorithms. It was designed by David wheeler and Roger Needham of the Cambridge computer laboratory in 1994. It has a kind of Feistel cipher structure which uses mixed algebraic operations such as XOR, ADD and shift to encrypt a plain text. This algorithm embeds confusion, diffusion properties in its implementation. It takes two 32 bits blocks of data which computes to 64 bits of data as input and encrypts it with 128 bit key at a time. It consists to 64 rounds, which is implemented in pairs termed as cycles(32 cycles). Though, 32 rounds of iterations is suggestable to obtain good ciper text. It can provide good dispersion just after 6 rounds of iterations. 16 rounds of iterations is sufficient for medium scale applications, through which it can provide good security. It provides high resistance to cryptanalysis operations and can achieve complete diffusion just after 6 rounds of Tea implementation. A magic constant is used in this algorithm which is 2654435769 or $9E3779B9_{16}$ is chosen to be $\lfloor 2^{32}/\phi \rfloor$, where ϕ is the golden ratio. The main operational logic of TEA is given below.

```
while (n-->0) {     /* basic cycle start */
sum += delta ;
 y += ((Z<<4)+k[0]) ^(Z+sum)^((Z>>5)+K[1]);
 Z += ((y<<4)+k[2]) ^(y+sum)^((y>>5)+K[3]);    /*end cycle*/
}
```

The routine relies on alternate use of XOR and ADD to provide non linearity. Dual shift causes all bits of key and data to be mixed repeatedly. It has a feistel type routine in which addition and substraction operations are used as reversible operators rather than XOR during decryption.

Differences between DES and TEA

DES is resource intensive algorithm, whereas TEA is small and at par has same encryption strength. TEA is easy to implement and highly portable when compared to DES. It can easily translate into many languages. TEA does not need S-boxes and P-boxes in its algorithm to provide diffusion and confusion properties. Speed is not a strong objective with TEA because it has 32 cycles (64 rounds) in algorithm, but on one implementation of TEA, it can provide three times as fast as a good software implementation when compared DES which has 16 rounds. TEA requires very little memory for its implementation when compared with DES. DES uses 64-bit key whereas TEA uses 128 bit key.

DES has 16 fixed rounds of operations included in its algorithm whereas number of rounds in TEA can be altered as per the requirement. DES requires permutation operations to be performed on its keys whereas TEA does not explicitly do any permutation of its key before using it in algorithm.

TASK-3

Below are the results when different sized input files have been passed to Tiny encryption algorithm and Data Encryption Standards algorithm. Results indicate the time taken to complete the operations in nano seconds. We could observe that as the file size increases, time taken to complete particular operation is also increased irrespective of mode of operation.

	Tiny Encryption Algorithm		DES	
	Ciper Block Chaining	Counter Mode	CiperBlockChaining	Counter Mode
encryption-64	709488	6535317	708595	702795
decryption-64	69163	5788347	415876	339126
encryption-512	2.26E+07	55272653	1339102	1231563
decryption-512	20837962	22939653	1027641	1107068
encryption-4096	5.49E+07	83152391	3727711	3344409
decryption-4096	41588913	127537757	2425198	1784428
encryption-32769	2.06E+08	603621332	8505819	8370615
decryption-32769	204839777	575961133	4020430	2819209

REFERENCES

- Tiny encryption algorithm basics from http://143.53.36.235:8080/tea.htm)
- wikipedia sources. https://en.wikipedia.org/wiki/Tiny_Encryption_Algorithm
- Andem, Vikram Reddy (2003). "A Cryptanalysis of the Tiny Encryption Algorithm, Masters thesis" (PDF). Tuscaloosa: The University of Alabama.

- web article at http://www.journaldev.com/1309/java-des-encryption-decryption-file-tutorial for java implementation of DES algorithm.