INFORMATION SECURITY

Class Assignment – 1

1) *What is the role of affine transform in AES S-Box*

A cryptographic function which satisfies above condition is said to be satisfying Strict Avalanche Criteria if and only if a one-bit change in input should result in exactly 50% change in the output bits. In this work we construct different S-boxes using Affine transformation and different irreducible polynomials for GF(2^8) and test them for Avalanche Criteria property

2) *AES and DES both use Feistel cipher structure. State true or false.*

False.

3) *Which is better AES or DES? Why?*

AES is better than DES because AES is more secure than DES cipher and is de facto world standard. DES can be easily broken as it has known vulnerabilities.

4) *List the way in which AES differs from DES.*

AES	DES
Byte-Oriented.	Bit-Oriented.
Key length can be 128-bits, 192-bits, and 256-bits.	The key length is 56 bits in DES.
Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)	DES involves 16 rounds of identical operations
The structure is based on a substitution-permutation network.	The structure is based on a substitution-permutation network.
AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.
AES can encrypt 128 bits of plaintext.	DES can encrypt 64 bits of plaintext.

5) *Why is DES deprecating?*

No major flaws were detected but was venerable to brute-force. The Data Encryption Standard's (DES) 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power. It no longer provides the security that is needed to protect federal government information.

6) *Draw the diagram elaborating the steps in one round of AES.*