Rebecca Dias 19
182027
TE CMPN A2

CSS

IAT-1

Q2)

a)

AES	DES
① AES stands for Advanced Encryption Standard	① DES stands for Data Encryption standard
② Key length from 128 bits, 192 bits to 256 bits	② Key length is of 56 bits
③ Rounds per key length: 128 bits – 10; 192 bits – 12; 256 bits – 14.	③ 16 rounds of identical operations,
④ AES structure is based on substitution permutation network	④ DES structure is based on feistal network
⑤ AES is de-facto world standard and is more structured than DES	⑤ DES is weak and 3DES is more secure than DES.
⑥ Byte substitution, Shift Row, Mix columns and key addition rounds	⑥ Expansion, XOR operation with round key, substitution and permutation rounds.
⑦ AES can encrypt 128 bits of plain text	⑦ DES can encrypt 64 bits of plain text.
⑧ AES derives from square cipher	⑧ DES derives from Lucifer cipher.

Rebecca Dias
182027 / 19
TE CMPN A2

CSS

DES (Data Encryption standard) is bit oriented and AES (Advanced Encryption Standard) is byte oriented.