Cryptography & Network Security
Quiz - I

Anish Sachdeva
DTU/2K16/MC/13

Q1) P = Hand over the briefcase to John.

Columns = 6 key = [3 5 1 6 2 4]

H A N D O V
E R T H E B
R I E F C A
S E T O J O
H N

Decrypting using the key

N O H V A D
T E E B R H
E C R A I F
T J S O E
H N O

C = NTETDECLJHERSHVBAOARIENDHFO

Q2) 8 50 keys

Q3) key =

N	O	N	D	E
R	I/J	S	T	H
B	G	I	N	F

W	O	N	D	E
R	I/J	S	T	H
B	G	N	F	M
A	C	K	L	P
Q	U	V	X	

W	O	N	D	E
R	I/J	S	T	H
B	G	F	M	A
C	K	L	P	Q
U	V	X	Y	Z

P = ATTACK POSTPONED

C

Q4) $26 + 3 = 29$

$\varphi(29) = p - 1 = 28$

Q5)

$(26+3)^{m^2}$ is key size

29^{m^2}

Q6) Caesar cipher, Hill cipher, Affine cipher, Playfair cipher, Autokey cipher, Vigenere cipher

Monoalphabetic, Polygraphic, Monoalphabetic, Polyalphabetic, Poly, Poly

Q7) MJQ done on google form

Q8) 2^{56} plaintext ciphertext pairs required to perform meet in the middle attack and solve with probability ~~$1 - 2^{-16}$~~ $1 - 2^{-16} \approx 1$

(Very high probability)

Q9) No, double encryption doesn't increase security as addition under $\mathbb{Z}_n$ forms a group and additions are equivalent to a single addition. eg.

$E_{K_1}(P) = (P + a) \bmod 26$ and $E_{K_2}(P) = (P + b) \bmod 26$

are 2 different encryption ciphers.

$E_2(E_1(p)) = ((p+a)+b) \bmod 26$

This is equivalent to $(p + (a+b)) \bmod 26$

Hence these 2 seperate encryptions can be turned into a single encryption.

$E_3(p) = [p + (a+b)] \bmod 26$

Hence no added security

Q9) Brute force for DES = 2^{55} per second = 2^{30}

$\frac{2^{55}}{2^{30}} = 2^{15}$ seconds = 32768 seconds

Q10) $110101 = (11)_2 (0101)_2 = (3)_{10} (5)_{10} = (9)_{10} = (001001)_2$

Q11) Expansion D-Box

Q12) Single letter frequency attack exploits the inherent characteristic of the language. In every language not all characters appear with the same frequency and some characters appear with higher frequency. In single letter frequency attack we measure the frequency of each letter and compare it with actual frequencies of letters in that language. e.g. E, T, A, O occur the most frequently in English language also