## Tudorial 6

Q1 Calculate ciphertext C1 & C2 for plaintest using Elgamal cryptosystem.

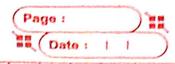
Consider public key = (2, 8, 11), prinate key = 3 & 2 = 4

y, = 9° mod p = 24 mod 11 = 16 mod 11

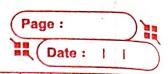
DG= 5

 $y_2 = /M \times e^{-2} \mod p$ = 7 × 84 mod 11 = 28 mod 11

C = (5,6)



22 Explain the process envolved in mossage digest generation & processing of single block in SHA-1. Padding: The input data is padded 20 shat its length is a multiple of 513 bils. The padding is done by add 1 bit followed by 0 bits 1 the length of input data in bits in a 64 bit representation Then the badded input is divided into 512 bit blocks & each block is further divided into 16 32-bit woulds initialised to a set of constant esing a compression function that operates on a set of 5 32-bit indermediate hosh values & the Bo word message schedule. After processing all blocks through different nounds to operations, the final hash value is obtained by and aniderals the five obtained bash values in register and somerting them to a fixed length message digest of 160 bits.



N	Date: 11
23	Graplain MAC based hash lunction
4	explain MAC based hash function with its design objectives & structures of the algorithm.
	of the also illem
	of the argonianon.
¥ = 2	MAC based hash function is a type of
	couptrarable bash worton that combines
-	cryptographic hash function that combines MAC code with a one-way hash function to broduce a secure message diagest The
9 1	to produce a secure message digest. The
	design objective of a MARC based
	désign objective of a MAC based hash function includés:
	Ser & Series Of Control of the Contr
	- To use hash hunchion that has form und
	in software & for which code is free
	Luidely anailable.
	a sail 2 de la contrata del contrata del contrata de la contrata del contrata del contrata de la contrata del contrata de la contrata del co
	> To allow for easy neplaceability of the
	embedded hash function in case forton or more secure hash function are
	or more secure hash Luntin or
+4	found are found or required.
	The state of the s
-	3 Structure of HMAC alexithm
	The working of HMAC & strets
	with taking a muse so Ma dain
	blocks of length 6 bits.
	An input signature is badded to
71.	the left of the message I whole
5 65/	is given as input to a hash tune
	United the state of the state o
	Was a second of the second of
	25104123