Q1 common prime = 71 primitive root 7 a) User A his a printe key Xa=5, Sind. public kep A= 75 mod 71 = 51 b) user 13 has a private key Xp=12 find public kep B=7" mod g1=4" 21 21 21 21 2 c) Shared secret key and shared so S=45 mod 7/ =35 2 3 S=51" mod 76 =35 2 D) 57 mod 71 = 25 5. 5/25 frod 7/0 = 1 = choose with = en 5= 25 th mod 71 = 57 So with our above example we can no longer guarantee that the calculated shoot key is the Same

Qx Our his been attempting to create a fraudulent where it's checksum value obtained from the hish function is the same as an original non - dangerous message. If the A signatured recipied is valid alea checksum of fraudulant message is equal to the checksum of the valid message, then the birthday attack has Succeeded and the from dulent message can be sent. B) For an M-bit message the affecter needs
2 min bits. This is because a high function generates 2 out pass, but due to the birthday () 2 1/2 = 232/20 = 212 = 4096 Seconds or about 68.26 Minutes. use 128 bit hash attacker needs 2 128/2 = 264 bits (c) 264/20 = 244 seconds = 565,59 h. 4 Vars

```
23 cipha-lest = dol 0111
   a = 1019, P = 1999

S = \{5, 9, 21, 45, 703, 215, 450, 946\} = 1794
    · is p > than ZS yes 1999 > 1794
       is gad [ 1999, [019] = 1? yes
      1999 = 1019 x1 +980
       10 19 = 980 x1 + 39
      980 = 25x 39 + 5
       39=7×5+4
5=4×1+1
                     ged of 1
       43 4x1+1
        So 4 $ pare coprime.
      B = { (5 x 1019) mod 1999 = 1097
            (9 x 1019) mod 1999 = 1175

(21 x 1019) mod 1999 = 1409

(45 x (019) mod 1999 = 1877

(1010 1019) mod 1999 = 1009
             (450, x(ds) mod 1489 = 1194
(450, x(ds) mod 1489 = 779
             (946 x low) mod 1499 - 45 6
        C=[1097.0]+[1175.1]+[1409.0]+[1877.8]
         + [1009 0] + [1194.1] + [779.1] + [456.1]
         C=5481
```

5481 - 1586	9 mad 1949 = 1665
	Parket Special Control of the Contro
1665-946	2 719
714 - 450	And the control of th
269-215	State Office in the Control of the C
54-45=	
9-9=0	CHES MORE CALCULATION AND AND AND AND AND AND AND AND AND AN
1	
(1)	its of I bit for printe key
check them	old 1111 which is correct.
ne ger	old DIII which is correct.
	h+ 2x + 2 / C
	It X is
So notes a la Setta	1 + 1 x 4 = 1
A CONTRACT BEACH .	
	977/92 20 1 4 1 66
	+ 60) = 666 [[10 [10 [10]] = 9
	CTIL = 284 Ind (1618 V)
	the second of th
	Potell a post los Colonial
	the second of th
	Potilis profiles (P. Dazit
	Potility of the control of the contr
	Potility position (Partition of the Partition of the Part