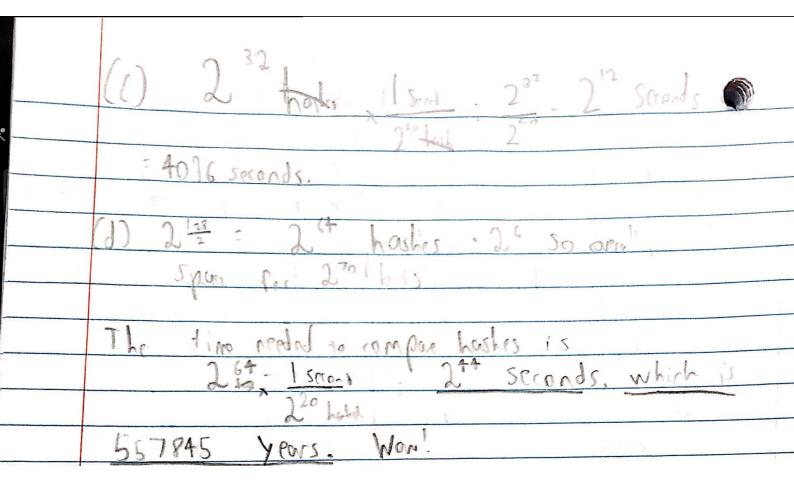
	Samuel Faroogvi 10/14/2018 HW 2.b
	(a) If XA:5, Ya: 75 mod 71:51 (b) If XB: 12, YB: 712 mod 71:4
	(c) The shored key is 51'2 mod 71 or 4'2 mod 71 : 58
	(d) - Finding the con root is very if you
	for say to find the solution to the
	discrete log problems. You would have to
	problem suggests, you would have x7 mod 71. You could find x = J27
	Very easly, therefore it is x mod 71:51.
0-2	that two values hash to the some hash
	Value. The attacker would be trying a bunch of values that he can generally and if any one valid, the attacker can said it
- 2 ^{E2}	to a client and the client would think
•	(b). It is a 6t-bit hugh code, so
	11 is 232 64 as the on 64 bite
	Messages. So, 15 232 to try everything, and store it, and the 64 (26) for early it ry.



(33) 1011.5 mod 1719= 1097 1011 · 21 mod 1979 1019.215" 1019-450" 1019.776 The inverse a mod p is equal to a p-2 mod p by
Fermat's littly theorem which is
1017 mod 1799: 1589 by Worlson Alpha 1097 1175 1409 1877 1009 1194 779 451 1175 + 1877 + 1194 + 779 + 456 = 5481 = W We figure out the plaintent by doing 1589.5481 mod 1999