

Homework 26, due November 6

- (1) What is the probability that there are two students in a class of 100 with university ID numbers that have the same last four digits?
- (2) Encode letters of the alphabet as integers mod 26, with  $A = 0$  and  $Z = 25$ . Encode a message  $m$  of letters as a list of numbers. For example, the message  $CAT$  becomes  $(2, 0, 19)$ . Define the hash  $H(m)$  to be the sum of the numbers making up  $m$ , modulo 26. Thus,  $H(CAT) = 2 + 0 + 19 \equiv 21 \pmod{26}$ .

Find two messages  $m$  and  $m'$  with the same hash value, where  $m$  is a message Alice would be willing to sign (e.g. "GOBYU") and the other is a message she would not want to sign (e.g. "IWILLPAYYOU TENDOLLARS").

- (3) Let Alice have public key  $(n, e) = (25957, 17)$ . Alice's corresponding private key is  $d = 13553$ . If  $m$  is one of the messages you found in problem 2, what is Alice's signature on  $H(m)$ ?