last name **first names** **id#**

---

c210W'16qz4 **45min** **closedbook** **page 1/1**

1. [5] DHM is an acronym for _____ _____ _____ , who found a solution to the problem of _____. This was a big problem in the 1970s, because _____

   _____

   Their method is practical: there is an efficient algorithm that takes as input numbers a, e, n and computes $x =$_____. Their method is secure: the best known algorithm for the inverse problem (given numbers a, x, n, find e such that _____) is little better than brute force.

2. [5] Here is Alice's public RSA info: modulus $t = 12916667$, exponent $z = 769$. Bob wants to send Alice the number $m = 3162453$ (with no hashing or signature). So he computes $v =$_____ and sends v to Alice. Alice knows the _____ numbers p, q such that _____, and has used the extended Euclid algorithm to find d satisfying this equation: _____ . To recover m, Alice evalutes this expression: $m =$_____ . What numbers does the eavesdropper Eve know? _____ . For this example, is it easy or hard for Eve to find m? Explain briefly. _____

   _____ .

3. [5] This is the _____ cryptosystem, developed by Feistel. 1) translate message into a string of _____. 2) split string into blocks of ____ digits, encrypt each block separately. 3) for each block, _____ the digits, then split into half-blocks Left0,Right0 each with ____digits; put digits in Right0 through a mangler _____ function; Right1 is mangled Right0 plus Left0; Left1 is original Right0; this is one round: there are _____ rounds in total. Mangler depends on a key agreed on by sender and receiver. _____ wanted the number of keys to be no more than 2^{56}, because _____ .

4. [5] Public-key cryptography uses _____ arithmetic, also known as clock arithemetic: if it is 2pm now, then 29 hours from now it will be _____pm, because `2 + 29 =` _____.

   The British kept public-key crypto research secret for many years. They had done the same with other crypto research, to their benefit: eg. _____. American public-key crypto research was made public. _____, _____, and _____ turned their p-kc system into a successful business. And _____ released a free p-kc system on the internet, because _____.