Midterm 1

7:00-9:00pm, 8 October

Notes: There are **five** *questions on this midterm. Answer each question part in the space below it, using the back of the sheet to continue your answer if necessary. If you need more space, use the blank sheet at the end. In both cases, be sure to clearly label your answers!* **None of the questions requires a very long answer, so avoid writing too much! Unclear or long-winded solutions may be penalized.** *The approximate credit for each question part is shown in the margin (total 100 points). Points are not necessarily an indication of difficulty!*

Your Name: **Your Section:**

Person on left: **Person on right:**

For official use; please do not write below this line! For official use; please do not write below this line!

Q1	16
Q2	20
Q3	20
Q4	14
Q5	15 + 15
Total	100

[exam starts on next page]

1. [Propositional Logic] [16 pts]

A. (8 pts - 2 pts each) State whether the following equivalences are valid or invalid. There is no need to justify your answers. Guess at your own risk - wrong answers will be awarded negative credit.

I. $\neg\forall n\,[(P(n) \wedge Q(n)) \Rightarrow \neg R(n)] \equiv \exists n\,[P(n) \wedge Q(n) \wedge R(n)]$

II. $\forall m\,\exists n\,[\forall l(A(m,l) \wedge B(n,l)) \Rightarrow C(m,n)] \equiv \forall m\,\exists n\,[\neg C(m,n) \Rightarrow \exists l(\neg A(m,l) \vee \neg B(n,l))]$

III. $\forall m\,\forall n\,[P(m) \Rightarrow Q(n)] \equiv \forall n\,\forall m\,[Q(n) \Rightarrow P(m)]$

IV. $\neg\forall l\,\exists m\,\forall n\,[(P(m) \wedge Q(l)) \vee R(m,n,l)] \equiv \exists l\,\forall m\,\exists n\,[(\neg P(m) \wedge \neg Q(l)) \vee \neg R(m,n,l)]$

B. (8 pts - 2 pts each) For nonnegative integers x and y, let $P(x,y)$ be the proposition that "$x + y > xy$" . Which of the following statements are true? Give a one line proof or a counterexample.

I. $\forall x\,\exists y P(x,y)$

II. $\exists x \, \exists y P(x, y)$

III. $\exists x \, \forall y P(x, y)$

IV. $\forall x \, \forall y P(x, y)$

2. [Proofs.] [20 pts]

A. (10 pts) Let D_n be the number of ways to tile a $2 \times n$ checkerboard with dominos, where a domino is a 1×2 piece. Prove that $D_n \leq 2^n$ for all positive integers n. (Find a recurrence relation for D_n. No need to give a proof. Then inductively prove the upper bound on D_n.)

Note that dominos can only be placed exactly aligned with checkerboard squares, and cannot be placed diagonally.

B. (10 pts) Show that $\forall$ odd $a \in N, a^2 = 1 \mod 8$.

3. [RSA] [20 pts]

A. (10 pts) $e = 7, p = 7, q = 11$ Find d.

B. (5 pts) With RSA Amazon can *sign* a message as follows; For a system with public key (N, e) and secret key d, Amazon sends the message $(x, x^d \mod N)$. If Bob gets (x, y), how can he verify that $y = x^d \mod N$? (Bob does not know d and the answer is very brief.)

C. (5 pts) Use the fact that $a^{p-1} = 1 \mod p$ for prime p and a relatively prime to p to prove that $a^{(p-1)(q-1)} = 1 \mod pq$ for primes p and q and a relatively prime to p and q.

4. [Stable Marriage] [14 pts]

A. (8 pts) Consider an instance of the Stable Marriage problem in which the men are $\{1, 2, 3, 4\}$, the women are $\{A, B, C, D\}$, and the preference lists are

Men (1-4)					Women (A-D)				
1:	A	B	D	C	A:	2	3	4	1
2:	C	B	A	D	B:	1	4	2	3
3:	D	C	B	A	C:	1	4	2	3
4:	D	C	A	B	D:	1	3	2	4

Use the traditional marriage algorithm to find the male-optimal pairing.

B. (3 pts) Given n men and n women, what is the minimum number of stable pairings that must exist for any set of preferences? Justify your answer by describing an instance.

C. (3 pts) We saw in the homework that it was possible for a pairing to be stable even if there was a pair (M, W) such that M was W's least favorite man and W was M's least favorite woman. What is the maximum number of couples with this property (each member is paired with their least favored partner) can there be in any stable pairing? Justify your answer.

5. [Codes] [30 pts]

A. (15 pts) Your friend sends you a message in the alphabet R = 0, F = 1, A = 2, U = 3, and N = 4 using the polynomial scheme discussed in class. Assume that a polynomial $P(\cdot)$ over $GF(q)$ is used, for the smallest value of q that will accommodate the given alphabet. The message size is 3. Four packets are sent where packet i (starting from 0) corresponded to $P(i)$. You receive the following packets.

- F
- U
- clearly corrupted
- N

Assuming the three decipherable packets arrive uncorrupted, what is the value in the corrupted packet? Justify your answer.

B. Say another message is sent using five packets and you receive packets F, U, N, U, and R, one of which is wrong.

I. (7 pts) The original message is either “FUN” or “RUN”. Which is it? Why? (Hint: try one.)

II. (4 pts) Recall that in the Berlekamp-Welch algorithm, one can set up a set of linear equations and use the solution to reconstruct the original polynomial. How many unknowns and equations do you have in the Berlekamp-Welch system for this situation?

III. (4 pts) Write out the equations that correspond to the first two received characters: i.e., $R(0)$ and $R(1)$. Denote the coefficients of $Q(x)$ using a_i and the coefficients of $E(x)$ by b_i.