COMP 170 – Fall 2006
Midterm 2 Solution

Q1. Bob is constructing an RSA key-pair. He first chooses $p = 11$, $q = 23$. He then calculates a private key d and a public key e. After choosing d he calculates $e = 147$. His public key is then the pair (n, e) where $n = pq = 253$.

Alice wants to send Bob some message M (where M is a positive integer < 253). She encrypts the message using the public key pair (n, e) =(253,147). The encrypted message she sends to Bob is the value $M' = 5$.
What is the value M that Bob reads after he decrypts the message?

To decrypt the encrypted message M' to get M, we need the private key d, which is the multiplicative inverse of $e = 147$ in Z_T, where $T = (p-1)(q-1) = 220$. In other words, we need d such that

$$ed \bmod T = 147d \bmod 220 = 1.$$

To decrypt the encrypted message M' to get M, we need the private key d, which is the multiplicative inverse of $e = 147$ in Z_T, where $T = (p-1)(q-1) = 220$. In other words, we need d such that

$$ed \bmod T = 147d \bmod 220 = 1.$$

Calculating this inverse, e.g., using the extended GCD algorithm, gives $d = 3$. M can then be computed as:

$$M = (M')^d \bmod n = 5^3 \bmod 253 = 125.$$

Q2. Consider the equations

$$\begin{aligned} x \bmod 27 &= 5 \\ x \bmod 68 &= 3 \end{aligned}$$

1. How many $x \in Z_{1836}$ solve both equations? Justify your answer.

Q2. Consider the equations

$$\begin{aligned} x \bmod 27 &= 5 \\ x \bmod 68 &= 3 \end{aligned}$$

1. How many $x \in Z_{1836}$ solve both equations? Justify your answer.

Since $\texttt{gcd}(27, 68) = 1$, the Chinese Remainder Theorem guarantees that there exists a unique solution for $x \in Z_{1836}$ $(1836 = 27 \cdot 68)$.

2. Give an $x \in Z_{1836}$ that solves both equations.

2. Give an $x \in Z_{1836}$ that solves both equations.

Let $m = 27$, $n = 68$, $a = 5$ and $b = 3$. We denote the multiplicative inverse of m in Z_n by $\overline{m}$ and that of n in Z_m by $\overline{n}$. The constructive proof for the Chinese Remainder Theorem taught in class gives the solution for x as

$$x = y \bmod 1836,$$

where

$$y = an\overline{n} + bm\overline{m}.$$

We can use the extended GCD algorithm to find $r, s \in Z$ that satisfy the following equation:

$$mr + ns = 27r + 68s = \mathtt{gcd}(27, 68) = 1.$$

Since $r = -5$ and $s = 2$ satisfy the equation, the inverses can be computed as

$$\begin{aligned} \overline{m} &= r \bmod n = (-5) \bmod 68 = 63 \\ \overline{n} &= s \bmod m = 2 \bmod 27 = 2. \end{aligned}$$

We can use the extended GCD algorithm to find $r, s \in Z$ that satisfy the following equation:

$$mr + ns = 27r + 68s = \mathtt{gcd}(27, 68) = 1.$$

Since $r = -5$ and $s = 2$ satisfy the equation, the inverses can be computed as

$$\begin{aligned} \overline{m} &= r \bmod n = (-5) \bmod 68 = 63 \\ \overline{n} &= s \bmod m = 2 \bmod 27 = 2. \end{aligned}$$

Hence we have

$$y = 5 \cdot 68 \cdot 2 + 3 \cdot 27 \cdot 63 = 5783$$

and

$$x = 5783 \bmod 1836 = 275.$$

3. Give an x such that x solves both equations and $3000 \leq x \leq 5000$.

3. Give an x such that x solves both equations and $3000 \leq x \leq 5000$.

$275 + k1836$ is a solution to the equation for all k. Letting $k = 2$ gives $x + 2 \cdot 1836 = 3947$, which is in the range $3000 \leq x \leq 5000$.

Q3. Answer the following questions. For parts (1)-(3) do not forget to justify your answers. For part (4) do not forget to show your calculations.

1. Is $(92^{100} \bmod 31) = (92^{10} \bmod 31)$?

Q3. Answer the following questions. For parts (1)-(3) do not forget to justify your answers. For part (4) do not forget to show your calculations.

1. Is $(92^{100} \bmod 31) = (92^{10} \bmod 31)$?

Yes. Since 31 is prime and 92 is not a multiple of 31, we can apply the corollary of Fermat's Little Theorem as follows:

$$92^{100} \bmod 31 = 92^{100 \bmod (31-1)} \bmod 31 = 92^{10} \bmod 31$$

So LHS $=$ RHS.

2. Is $(80^{491} \bmod 71) = (74^{492} \bmod 71)$?

2. Is $(80^{491} \bmod 71) = (74^{492} \bmod 71)$?

Yes.

$$\begin{aligned}\text{LHS} &= 80^{491} \bmod 71 = 9^{491} \bmod 71 = 9^{491 \bmod 70} \bmod 71 = 9 \bmod 71.\\ \text{RHS} &= 74^{492} \bmod 71 = 3^{492} \bmod 71 = 3^{492 \bmod 70} \bmod 71 = 3^{2} \bmod 71 = 9 \bmod 71.\end{aligned}$$

Hence LHS $=$ RHS.

2. Is $(80^{491} \bmod 71) = (74^{492} \bmod 71)$?

Yes.

$$\begin{aligned}
\text{LHS} &= 80^{491} \bmod 71 = 9^{491} \bmod 71 = 9^{491 \bmod 70} \bmod 71 = 9 \bmod 71. \\
\text{RHS} &= 74^{492} \bmod 71 = 3^{492} \bmod 71 = 3^{492 \bmod 70} \bmod 71 = 3^{2} \bmod 71 = 9 \bmod 71.
\end{aligned}$$

Hence LHS $=$ RHS.

3. Is $(24^{56} \bmod 72) = (31^{56} \bmod 72)$?

2. Is $(80^{491} \bmod 71) = (74^{492} \bmod 71)$?

Yes.

$$\begin{aligned} \mathrm{LHS} &= 80^{491} \bmod 71 = 9^{491} \bmod 71 = 9^{491 \bmod 70} \bmod 71 = 9 \bmod 71. \\ \mathrm{RHS} &= 74^{492} \bmod 71 = 3^{492} \bmod 71 = 3^{492 \bmod 70} \bmod 71 = 3^{2} \bmod 71 = 9 \bmod 71. \end{aligned}$$

Hence LHS $=$ RHS.

3. Is $(24^{56} \bmod 72) = (31^{56} \bmod 72)$?

No.

$$\mathrm{LHS} = 24^{56} \bmod 72 = (24^{2})^{28} \bmod 72 = (576 \bmod 72)^{28} \bmod 72 = 0.$$

Alternatively, one can note that $24 = 2^{3}3$ so $72 = 2^{3}3^{2} | 24^{56}$ so $\mathrm{LHS} = 0$.

RHS: since any integral power of an odd integer is odd, 31^{56} is odd.

Hence $31^{56} \bmod 72$ is an odd number, which can't be equal to 0 (LHS).

4. What is the value of $2^{2050} \bmod 62$?

4. What is the value of $2^{2050} \bmod 62$?

Use *Repeated squaring*.
Note that

$$2^{2050} \bmod 62 = (2^{2048} \cdot 2^2) \bmod 62 = (2^{2^{11}} \cdot 2^{2^1}) \bmod 62.$$

Let $I_0 = 2$ and $I_i = (I_{i-1} \cdot I_{i-1}) \bmod 62 = 2^{2^i} \bmod 62$ for $1 \le i \le 11$, i.e.

$$I_1 = 4, I_2 = 16, I_3 = 8, I_4 = 2, I_5 = 4, I_6 = 16,$$

$$I_7 = 8, I_8 = 2, I_9 = 4, I_{10} = 16, I_{11} = 8.$$

4. What is the value of $2^{2050} \bmod 62$?

Use *Repeated squaring*.
Note that

$$2^{2050} \bmod 62 = (2^{2048} \cdot 2^2) \bmod 62 = (2^{2^{11}} \cdot 2^{2^1}) \bmod 62.$$

Let $I_0 = 2$ and $I_i = (I_{i-1} \cdot I_{i-1}) \bmod 62 = 2^{2^i} \bmod 62$ for $1 \le i \le 11$, i.e.

$$I_1 = 4, I_2 = 16, I_3 = 8, I_4 = 2, I_5 = 4, I_6 = 16,$$

$$I_7 = 8, I_8 = 2, I_9 = 4, I_{10} = 16, I_{11} = 8.$$

Hence

$$(2^{2^{11}} \cdot 2^{2^1}) \bmod 62 = (I_{11} \cdot I_1) \bmod 62 = 32.$$

Q4. Use induction to prove the truth of the following statements about integers.

1. $$\forall n \geq 0, \quad \left(\frac{5}{3}\right)^n = \sum_{i=0}^{n} \binom{n}{i} \left(\frac{2}{3}\right)^i$$

Q4. Use induction to prove the truth of the following statements about integers.

1.

$$\forall n \geq 0, \quad \left(\frac{5}{3}\right)^n = \sum_{i=0}^{n} \binom{n}{i} \left(\frac{2}{3}\right)^i$$

Let $a = 2/3$. The statement can be rewritten as

$$(1 + a)^n = \sum_{i=0}^{n} \binom{n}{i} a^i.$$

So essentially we are proving a special case of the Binomial Theorem.

Base case: Let $n = 0$. LHS $= 1$ and RHS $= 1$. So the statement is true for the base case.

Base case: Let $n = 0$. LHS $=$ 1 and RHS $=$ 1. So the statement is true for the base case.

Inductive case: Let $n > 0$ and that the statement is true for $n - 1$, i.e.,

$$(1+a)^{n-1} = \sum_{i=0}^{n-1} \binom{n-1}{i} a^i.$$

Using this inductive hypothesis and Pascal's relationship $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$ we get

$$
\begin{aligned}
LHS &= (1+a)\cdot(1+a)^{n-1} \\
&= (1+a)\sum_{i=0}^{n-1}\binom{n-1}{i}a^{i} \\
&= \sum_{i=0}^{n-1}\binom{n-1}{i}a^{i} + \sum_{i=0}^{n-1}\binom{n-1}{i}a^{i+1} \\
&= \sum_{i=0}^{n-1}\binom{n-1}{i}a^{i} + \sum_{i=1}^{n}\binom{n-1}{i-1}a^{i} \\
&= \binom{n-1}{0}a^{0} + \sum_{i=1}^{n-1}\binom{n-1}{i}a^{i} + \sum_{i=1}^{n-1}\binom{n-1}{i-1}a^{i} + \binom{n-1}{n-1}a^{n} \\
&= \binom{n}{0}a^{0} + \sum_{i=1}^{n-1}\binom{n}{i}a^{i} + \binom{n}{n}a^{n} \\
&= RHS
\end{aligned}
$$

Based on the weak principle of mathematical induction, we conclude that the statement is true for all integers $n \geq 0$.

Based on the weak principle of mathematical induction, we conclude that the statement is true for all integers $n \geq 0$.

Alternatively, one can muliply both sides of the original equation by 3^n to see that it is equivalent to

$$\forall n \geq 0, \quad 5^n = (2+3)^n = \sum_{i=0}^{n} \binom{n}{i} 2^i 3^{n-i},$$

which is also a special case of the Binomial Theorem and then prove this special case.

2. Let $T(n)$ be defined by

$$T(n) = \begin{cases} 1 & \text{if } n = 0 \\ 1 + 2n - n^2 + 2\sum_{i=0}^{n-1} T(i) & \text{if } n > 0. \end{cases}$$

Then $\forall n \geq 0,\ T(n) = 3^n + n.$

2. Let $T(n)$ be defined by

$$T(n) = \begin{cases} 1 & \text{if } n = 0 \\ 1 + 2n - n^2 + 2\sum_{i=0}^{n-1} T(i) & \text{if } n > 0. \end{cases}$$

Then $\forall n \geq 0,\ T(n) = 3^n + n.$

Base case: Let $n = 0$. $T(0) = 3^0 + 0 = 1$. So the base case is true.

Inductive case: Let $n > 0$ and $T(i) = 3^i + i$, $0 \leq i < n$.

$$
\begin{aligned}
T(n) &= 1 + 2n - n^2 + 2\sum_{i=0}^{n-1} T(i) \\
&= 1 + 2n - n^2 + 2\sum_{i=0}^{n-1} (3^i + i) \\
&= 1 + 2n - n^2 + 2\left(\sum_{i=0}^{n-1} 3^i + \sum_{i=0}^{n-1} i\right) \\
&= 1 + 2n - n^2 + 2\left(\frac{3^n - 1}{3 - 1} + \frac{n(n-1)}{2}\right) \\
&= 1 + 2n - n^2 + 3^n - 1 + n^2 - n \\
&= 3^n + n.
\end{aligned}
$$

Inductive case: Let $n > 0$ and $T(i) = 3^i + i$, $0 \leq i < n$.

$$\begin{aligned}
T(n) &= 1 + 2n - n^2 + 2\sum_{i=0}^{n-1} T(i) \\
&= 1 + 2n - n^2 + 2\sum_{i=0}^{n-1}(3^i + i) \\
&= 1 + 2n - n^2 + 2\left(\sum_{i=0}^{n-1} 3^i + \sum_{i=0}^{n-1} i\right) \\
&= 1 + 2n - n^2 + 2\left(\frac{3^n - 1}{3 - 1} + \frac{n(n-1)}{2}\right) \\
&= 1 + 2n - n^2 + 3^n - 1 + n^2 - n \\
&= 3^n + n.
\end{aligned}$$

Based on the strong principle of mathematical induction, we conclude that the statement is true for all integers $n \geq 0$.

Q5. Find all values $n \in Z^+$ such that

$$3^n < 10 + n!.$$

Justify the correctness of your answer.

Q5. Find all values $n \in Z^+$ such that

$$3^n < 10 + n!.$$

Justify the correctness of your answer.

Let us **check a few of the smallest positive integers**:

$$\begin{aligned}
n = 1: &\qquad 3 < 10 + 1 \\
n = 2: &\qquad 9 < 10 + 2 \\
n = 3: &\qquad 27 > 10 + 6 \\
n = 4: &\qquad 81 > 10 + 24 \\
n = 5: &\qquad 243 > 10 + 120 \\
n = 6: &\qquad 729 < 10 + 720
\end{aligned}$$

We **guess** that the statement holds for all integers $n \geq 6$. We prove this by induction on $n \geq 6$.

Base case: Already proved above.

Base case: Already proved above.

Inductive case: Let $n > 6$ and that the statement is true for $n-1$, i.e.,

$$3^{n-1} < 10 + (n-1)!.$$

Since

$$3^n = 3 \cdot 3^{n-1} < 30 + 3(n-1)!,$$

we want to prove that

$$30 + 3(n-1)! < 10 + n!.$$

To prove this, it suffices to show that

$$n! - 3(n-1)! = (n-3)(n-1)! > 20.$$

Since $n > 6$ (or $n \geq 7$),

$$(n-3)(n-1)! \geq 4 \cdot 6! > 20.$$

Hence we can conclude that the statement is true for all positive integers except for $n \in \{3, 4, 5\}$.

Q6. Consider this natural language (i.e., English) sentence:

for all integers a, b and c, if $(a - b)$ and $(b - c)$ are both even,
then $(a - c)$ is also even.

Let $p(x)$ denote the statement "x *is even*". In the two subproblems below you are asked to express the above sentence using $p(x)$, quantifiers, logical connectives and implications

1. Express the sentence *without* using the logical OR ($\vee$) connective.

$$\forall a \in Z\ (\forall b \in Z\ (\forall c \in Z\ ((p(a-b) \wedge p(b-c)) \Rightarrow p(a-c)\ )\ )\ )$$

$$\forall a \in Z\ (\forall b \in Z\ (\forall c \in Z\ ((p(a-b) \wedge p(b-c)) \Rightarrow p(a-c)\ )\ )\ )$$

2. Express the sentence using *only* $p(x)$, quantifiers, negations and the logical OR ($\vee$) connective (you may not use any other logical connectives or implications).

$$\forall a \in Z\ (\forall b \in Z\ (\forall c \in Z\ ((p(a-b) \wedge p(b-c)) \Rightarrow p(a-c)\ )\ )\ )$$

2. Express the sentence using *only* $p(x)$, quantifiers, negations and the logical OR ($\vee$) connective (you may not use any other logical connectives or implications).

Start from the equation above and use the fact that $p \Rightarrow q$ is equivalent to $\neg p \vee q$ and DeMorgan's laws to get

$$\begin{aligned}
& \forall a \in Z\ (\forall b \in Z\ (\forall c \in Z\ ((p(a-b) \wedge p(b-c)) \Rightarrow p(a-c)\ )\ )\ ) \\
= \ & \forall a \in Z\ (\forall b \in Z\ (\forall c \in Z\ (\neg(p(a-b) \wedge p(b-c)) \vee p(a-c)\ )\ )\ ) \\
= \ & \forall a \in Z\ (\forall b \in Z\ (\forall c \in Z\ (\neg p(a-b) \vee \neg p(b-c) \vee p(a-c)\ )\ )\ )
\end{aligned}$$

Q7. Construct a contrapositive proof that for all integers x,

If $(1 + x^7)$ is even, then x is odd.

Q7. Construct a contrapositive proof that for all integers x,

If $(1 + x^7)$ is even, then x is odd.

Let $p(x)$ denote "$(1+x^7)$ is even" and $q(x)$ denote "x is odd". The statement can be represented as:

$$p(x) \Rightarrow q(x),$$

which is logically equivalent to

$$\neg q(x) \Rightarrow \neg p(x).$$

To construct a contrapositive proof, we first assume that $\neg q(x)$ is true, i.e., x is not odd or x is even. So there exists an integer $k \in Z$ such that $x = 2k$. Thus we can rewrite $1 + x^7$ as

$$1 + x^7 = 1 + 2^7 k^7 = 1 + 2(2^6 k^7),$$

which obviously is an odd number, i.e., $\neg p(x)$. Hence the original statement $p(x) \Rightarrow q(x)$ is correct.

Q8. Consider the following quantified statement about elements in some universe U :

$$\forall x \in U \ (\exists y \in U \ (P(x,y) \vee Q(x,y) \ ) \ ) \qquad (1)$$

Let $R(x,y) = \neg P(x,y)$ and $S(x,y) = \neg Q(x,y)$. Express the negation of the statement in Equation (1) in terms of $R(x,y)$ and $S(x,y)$. The negation sign ($\neg$) should *not* appear in your statement. Show how you derived your new statement.

Using the facts

- $\neg\forall x \in U\ (p(x))$ is equivalent to $\exists x \in U\ (\neg p(x))$
- $\neg\exists x \in U\ (p(x))$ is equivalent to $\forall x \in U\ (\neg p(x))$
- DeMorgan's laws

we get

$$\begin{aligned}
& \neg\forall x \in U\ \ (\exists y \in U\ \ (P(x,y) \vee Q(x,y)\ )\ ) \\
= \quad & \exists x \in U\ \ (\neg\exists y \in U\ \ (P(x,y) \vee Q(x,y)\ )\ ) \\
= \quad & \exists x \in U\ \ (\forall y \in U\ \ \neg(P(x,y) \vee Q(x,y)\ )\ ) \\
= \quad & \exists x \in U\ \ (\forall y \in U\ \ (\neg P(x,y) \wedge \neg Q(x,y)\ )\ ) \\
= \quad & \exists x \in U\ \ (\forall y \in U\ \ (R(x,y) \wedge S(x,y)\ )\ )
\end{aligned}$$

Q9.

1. Consider the recurrence below defined on $n \geq 0$.

$$T(n) = \begin{cases} 2 & \text{if } n = 0 \\ 4T(n-1) + 7 & \text{if } n > 0 \end{cases}$$

Give a closed-form, exact solution to the recurrence.

You only have to give the solution. You do not need to show how you derived it.

From the theorem proved in class or just by iterating the recurrence, we have

$$T(n) = r^n b + a\frac{r^n - 1}{r - 1},$$

where $T(n) = rT(n-1) + a$, $T(0) = b$ and $r \neq 1$. Substituting $r = 4$, $a = 7$ and $b = 2$ into the equation, we have

$$T(n) = 2 \cdot 4^n + 7\frac{4^n - 1}{4 - 1} = \frac{13 \cdot 4^n - 7}{3}.$$

2. Now, prove the correctness of your solution by induction.

2. Now, prove the correctness of your solution by induction.

Base case: Let $n = 0$. $T(0) = (13 - 7)/3 = 2$. So the base case is true.

2. Now, prove the correctness of your solution by induction.

Base case: Let $n = 0$. $T(0) = (13 - 7)/3 = 2$. So the base case is true.

Inductive case: Let $n > 0$ and that the statement is true for $n - 1$, i.e.,

$$T(n-1) = \frac{13 \cdot 4^{n-1} - 7}{3}.$$

$$\begin{aligned}
T(n) &= 4T(n-1) + 7 \\
&= 4 \cdot \frac{13 \cdot 4^{n-1} - 7}{3} + 7 \\
&= \frac{13 \cdot 4^{n} - 28}{3} + 7 \\
&= \frac{13 \cdot 4^{n} - 7}{3}.
\end{aligned}$$

2. Now, prove the correctness of your solution by induction.

Base case: Let $n = 0$. $T(0) = (13 - 7)/3 = 2$. So the base case is true.

Inductive case: Let $n > 0$ and that the statement is true for $n - 1$, i.e.,

$$T(n-1) = \frac{13 \cdot 4^{n-1} - 7}{3}.$$

$$\begin{aligned}
T(n) &= 4T(n-1) + 7 \\
&= 4 \cdot \frac{13 \cdot 4^{n-1} - 7}{3} + 7 \\
&= \frac{13 \cdot 4^{n} - 28}{3} + 7 \\
&= \frac{13 \cdot 4^{n} - 7}{3}.
\end{aligned}$$

Based on the weak principle of mathematical induction, we conclude that the statement is true for all integers $n \geq 0$.