MATH/CMSC 456, Jeffrey Adams FINAL May 18, 2005
SOLUTIONS

1. [25 points]
   (a) Hill Cipher YES
   (b) RSA NO
   (c) Affine Cipher YES
   (d) DES NO
   (e) Vigenère YES

2. [30]
   (a) There is no decryption function, since the function is not invertible. The problem is $(4, 50) = 2 \neq 1$ so f^{-1} does not exist, since it would have to satisfy $f^{-1}(y) = 4^{-1}(x - 20) \pmod{50}$.
   (b) We have $28 = 4x + 20$, or $4x = 8 \pmod{50}$. Divide both sides by $(4, 50) = 2$ to give $2x = 4 \pmod{25}$. So $x = 2$ or $25 + 2 = 27 \pmod{50}$.
   Alternatively, obviously 2 is a solution. Then since $4 \times 25 = 0 \pmod{50}$, we can add any multiple of 25 to this. But adding 50 doesn't change the answer $\pmod{50}$, so the two solutions are 2 and 27.
   (c) We have $y = 4x + 20 \pmod{50}$, so $17 = 4x + 20$, or $4x = -3 \pmod{50}$. Since 3 is no divisible by $(4, 50) = 2$ this has not solutions. (To be explicit, if $4x = -3 \pmod{50}$, then $4x = -3 + 50k$ for some integer k. Then $-3 = 4x - 50k$; the right hand side is divisible by 2 and the left hand side isn't, a contradiction.)

3. [30]
   (a) We must have $(e, \phi(n)) = 1$. Note that $\phi(pqr) = n(1 - \frac{1}{p})(1 - q\frac{1}{q})(1 - r\frac{1}{r}) = (p-1)(q-1)(r-1)$. So we must have $(e, (p-1)(q-1)(r-1)) = 1$.
   (b) Solve $de = 1 \pmod{(p-1)(q-1)(r-1)}$. This we can do by (a).

4. [30]
   (a) This is the $p - 1$ factorization method, which works since $p - 1$ has all small factors. Note that 35! has 32 powers of 2. That is, it contains $2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34$, for a total of $1+2+1+3+1+2+1+4+1+2+1+3+1+2+1+5+1 = 32$ factors of 2. It is also obviously divisibly by 3. So $p - 1 | 35!$, i.e. $35! = (p-1)k$ for some integer k. Then $2^{35!} = 2^{k(p-1)} = (2^{p-1})^k = 1 \pmod{p}$ by Fermat.

(b) Compute $(2^{35!}-1, n)$. Since $2^{35!} = 1 \pmod{p}$, $p|2^{35!}-1$. Also $q-1$ does not divide 35! since $53|q-1$. So $2^{35!} \neq 1 \pmod{q}$. Therefore$(2^{35!}-1, n) = p$.

5. [30]

(a) Compute

$$\begin{aligned}\beta^r r^s &= \beta^r(\beta^v\alpha^u)^{-rv^{-1}} \\ &= \beta^r\beta^{-r}\alpha^{-ruv^{-1}} \\ &= \alpha^{(-rv^{-1})u} \\ &= \alpha^{su} \\ &= \alpha^m\end{aligned}$$

(everything is $\mod n$).

(b) No, she has to pick u, v first and then m.

(c) Again since she picks r, s first, and then u, she would have to solve $h(m) = su \pmod{p-1}$. But this isn't possible with a hash function.

6. [15] The key is $2^{xy} \pmod{p} = 2^{21} \pmod{29} = (2^5)^4 \times 2 \pmod{35}$, or $3^4 \times 2 \pmod{35} = 81 \times 2 = 46 = 17 \pmod{29}$.

7. (a) This is $P + (-P) = \infty$.

(b) Since ∞ is like 0, this is $(9, 10)$.

(c) First of all $m = (12-4)/(7-2) = 8/5 \pmod{31}$. We need $5^{-1} \pmod{35}$. Clearly $5 \times 6 = -1 \pmod{31}$, so $5^{-1} = -6 = 25 \pmod{31}$. So $m = 8 \times 25 = 200 = 14 \pmod{31}$, and $x_3 = 14^2-2-7 = 1 \pmod{31}$. Then $y_3 = 14(2-1)-4 = 10 \pmod{31}$. So the solution is $(1, 10)$.

(d) Solve $y^2 = 8^3 + 16 + 4 = 5 \pmod{31}$. This is easy: $31 + 5 = 36$, so $y = 6$ is a solution. So there are exactly two solutions $y = \pm 6$.

(e) Solve $y^2 = 5^3+10+b \pmod{223676221} = 135+b \pmod{223676221}$. So we just need $b+135$ is a square $\pmod{223676221}$. For example take $b = 9$ so $y^2 = 144$, i.e. $y = \pm 12$. You could also take $b = -14 \pmod{223676221}$, so $y^2 = 121$, i.e. $y = \pm 11$. Note that p is mostly irrelevant here.