1.27 Consider an RSA key set with $p=17$, $q=23$, $N=391$, $e=3$. What value of d should be used for the secret key? What is the encryption of the message $M=41$?

d is the inverse of e mod $(p-1)(q-1)$ 235

inverse of 3 mod $16 \cdot 22$

$\text{extEuclid}(352, 3) \rightarrow \text{extEuclid}(3,1) \rightarrow \text{extEuclid}(1,0) = (1,0,1)$

So, $\text{extEuclid}(3,1) = (0,1,1)$

$\text{extEuclid}(352,3) = (1,-117,1)$

$352(1) + 3(-117) = 1$

$-117 + 352 = 235$

$\boxed{d = 235}$

$M=41$

The encryption of 41 is $y = 41^3 \bmod 391$

$\underline{y = 105}$

1.28 In an RSA cryptosystem, $p=7$ and $q=11$. Find appropriate exponents d and e.

e should be relatively prime to $(p-1)(q-1)$

$\gcd(e, (p-1)(q-1)) = 1$

$\gcd(7, 60) = 1$ ✓

$\boxed{e = 7}$

d is the inverse of $7 \bmod 60$

$7x \equiv 1 \bmod 60$

$\text{extEuclid}(60,7) \to \text{extEuclid}(7,4) \to \text{extEuclid}(4,3) \to \text{extEuclid}(3,1)$

$\to \text{extEuclid}(1,0)$ $\quad (x', y', d) = (1, 0, 1)$

So, $\text{extEuclid}(3,1) = (0, 1, 1)$

$\text{extEuclid}(4,3) = (1, -1, 1)$

$\text{extEuclid}(7,4) = (-1, 2, 1)$

$\text{extEuclid}(60,7) = (2, -17, 1)$

$60(2) + 7(-17) = 1$

$-17 + 60 = \boxed{43 = d}$

1.29 a) We can assume that the first two elements of some random tuple (x_1, x_2, x_3) are the same as the first two elements of another random tuple (y_1, y_2, y_3) and $x_3 \neq y_3$. The tuples hash to the same value if and only if the following expression is true:

$$\sum_{i=1}^{2} a_i (x_i - y_i) \equiv a_3 (y_3 - x_3) \pmod m$$

Let the value on the left side be equal to some value c. Then,

$c \equiv a_3(y_3 - x_3) \pmod m$. The following must be true: $a_3 \equiv c(y_3 - x_3)^{-1}$

Since m is prime and $x_3 \neq y_3$, there is a distinct value of $(y_3 - x_3)^{-1}$

(mod m). and c modulo m is distinct. Therefore, the probability of choosing a_3 in such a way is $\frac{1}{m}$. This hashing function is universal and three random bits are required to choose a function from this family.

b) This change is no longer universal because m is not prime and $(y_1-x_1)^{-1}$ may no longer exist. And three random bits are required to choose a function from this family

c) This function is not universal because the probability of two inputs a and b to hash the same thing is not $\frac{1}{m}$.

1.31 Consider the problem of computing $N! = 1 \cdot 2 \cdot 3 \cdots N$

a) If N is an n-bit number, N! is approximately $\Theta(N \log_2 N)$ bits long

b)

```
Factorial(N)
if N equals 0
    return 1
return N*Factorial(N-1)
```

The algorithm has N iterations which makes the time complexity $O(N)$. Each multiplication takes nm time therefore the algorithm has a running time of $O(N \cdot nm)$

1.31 modified: $O(N \cdot n \cdot m^{0.585})$

2.4 Algorithm A: $a=5$ $b=2$ $d=1$

$T(n)=5T\left(\frac{n}{2}\right)+O(n)$

$\log_b a=\log_2 5>d \Rightarrow O\left(n^{\log_2 5}\right)$

Algorithm B:

$T(n)=2T(n-1)+O(1)$

$T(1)=1$

$T(3)=2T(2)+2\cdot 2\cdot T(1)+c$

$T(4)=2T(3)+2\cdot 2\cdot 2\cdot T(2)+2\cdot 2\cdot T(1)+c$ $O(2^n)$

Algorithm C: $a=9$ $b=3$ $d=2$

$T(n)=9\cdot T\left(\frac{n}{3}\right)+O(n^2)$

$\log_b a=\log_3 9=d \Rightarrow O(n^2\log n)$

I would Choose Algorithm C

2.5 a) $T(n)=2T\left(\frac{n}{3}\right)+1$ $a=2$ $b=3$ $d=0$

$\log_b a=\log_3 2>d \Rightarrow \boxed{O\left(n^{\log_3 2}\right)}$

b) $T(n)=5T\left(\frac{n}{4}\right)+n$ $a=5$ $b=4$ $d=1$

$\log_a b=\log_4 5>d \Rightarrow \boxed{O\left(n^{\log_4 5}\right)}$

c) $T(n)=7T\left(\frac{n}{7}\right)+n$ $a=7$ $b=7$ $d=1$

$\log_a b = \log_7 7 = d \Rightarrow \boxed{O(n \log n)}$

d) $T(n) = 9T\left(\frac{n}{3}\right) + n^2$ $a = 9$ $b = 3$ $d = 2$

$\log_b a = \log_3 9 = d \Rightarrow \boxed{O(n^2 \log n)}$

e) $T(n) = 8T\left(\frac{n}{2}\right) + n^3$ $a = 8$ $b = 2$ $d = 3$

$\log_b a = \log_2 8 = d \Rightarrow \boxed{O(n^3 \log n)}$

f) $T(n) = 49T\left(\frac{n}{25}\right) + n^{3/2} \log n$ $a = 49$ $b = 25$ $d = \frac{3}{2} \log n$

$\log_b a = \log_{25} 49 > d \Rightarrow \boxed{O(n^{\log_{25}(49)})}$

g) $T(n) = T(n-1) + 2$

$T(n-1) = T((n-1)-1) + 2$

$T(n-1) = T(n-2) + 2$

$T(n) = T(n-2) + 2 + 2$

$T(n) = T(n-2) + 4$

$T(n-2) = T((n-2)-1) + 2$

$T(n-2) = T(n-3) + 2$

$T(n) = T(n-3) + 2 + 4$

$T(n) = T(n-3) + 6$

General pattern: $T(n) = T(n-k) + kc$ $k = n$

$T(n) = T(0) + nc$ $T(0) = 2$

$T(n) = 2 + nc$

$\boxed{T(n) = O(n)}$

h) $T(n) = T(n-1) + n^c \quad c \geq 1$

$T(n-1) = T((n-1)-1) + n^c$

$T(n-1) = T(n-2) + n^c$

$T(n) = T(n-2) + 2n^c$

$T(n-2) = T((n-2)-1) + n^c$

$T(n-2) = T(n-3) + n^c$

$T(n) = T(n-3) + 3n^c$

General pattern: $T(n) = T(n-k) + kn^c$ substitute $k = n$

$T(n) = T(0) + n \cdot n^c$

$T(n) = n^{c+1}$

$\boxed{T(n) = O(n^{c+1})}$

i) $T(n) = T(n-1) + c^n \quad c > 1$

$T(n-1) = T((n-1)-1) + c^{n-1}$

$T(n-1) = T(n-2) + c^{n-1}$

$T(n) = T(n-2) + c^{n-1} + c^n$

$T(n-2) = T((n-2)-1) + c^{n-2}$

$T(n-2) = T(n-3) + c^{n-2}$

$T(n) = T(n-3) + c^{n-2} + c^{n-1} + c^n$

General pattern : $T(n) = T(n-k) + \sum_{i=1}^{n} c^i$ substitute $k=n$

$$T(n) = T(0) + \sum_{i=1}^{n} c^i$$

$$T(n) = \frac{c^n - 1}{c-1} \quad \boxed{T(n) = O(c^n)}$$

j) $T(n) = 2T(n-1) + 1$

$T(n-1) = 2T((n-1)-1) + 1 = 2T(n-2) + 1$

$T(n) = 2(2T(n-2)+1) + 1$

$T(n) = 4T(n-2) + 2 + 1 = 4T(n-2) + 3$

$T(n-2) = 2T((n-2)-1) + 1 = 2T(n-3) + 1$

$T(n) = 4(2T(n-3)+1) + 3 = 8T(n-3) + 7$

General pattern : $T(n) = 2^k T(n-k) + (2^k - 1)$ substitute $k=n$

$$T(n) = 2^n T(0) + (2^n - 1) \quad T(0) = 1$$

$$T(n) = 2^n + 2^n - 1$$

$$\boxed{T(n) = O(2^n)}$$

k) $T(n) = T(\sqrt{n}) + 1$ Assume $n = 2^m$ $m = \log n$

$T(2^m) = T(2^{m/2}) + 1$

$S(m) = S(\frac{m}{2}) + 0$ $a=1$ $b=2$ $d=0$

$\log_b a = \log_2 1 = d \Rightarrow S(m) = O(m^c \log m)$

$S(m) = O(\log m)$ $m = \log n$

$$\boxed{T(n) = O(\log \log n)}$$

2.8) a) $(1,0,0,0)$ $\omega = e^{\frac{2\pi i}{4}} = e^{\frac{\pi i}{2}} = \cos\frac{\pi}{2} + i\cdot\sin\frac{\pi}{2} = 0 + i = i$

$\boxed{\omega = i}$

$FFT([1,0,0,0], i)$ $n=4$

$(s_0, s_1) = FFT([1,0], i^2) = FFT([1,0], -1)$

$FFT([1,0], -1)$ $n=2$ $\Rightarrow (1,1)$

$s_0 = FFT(1,1) = 1$ $r_0 = s_0 + \omega^0 s'_0 = 1+0 = 1$

$s'_0 = FFT(0,1) = 0$ $r_1 = s_0 - \omega^0 s'_0 = 1-0 = 1$

$(s'_0, s'_1) = FFT([0,0], i^2) = FFT([0,0], -1)$

$FFT([0,0], -1)$ $n=2$ $\Rightarrow (0,0)$

$s_0 = FFT(0,1) = 0$ $r_0 = s_0 + \omega^0 s'_0 = 0+0 = 0$

$s'_0 = FFT(0,1) = 0$ $r_1 = s_0 - \omega^0 s'_0 = 0 - 0 = 0$

$s_0 = 1$ $r_0 = s_0 + \omega^0 s'_0 = 1+0 = 1$

$s_1 = 1$ $r_2 = s_0 - \omega^0 s'_0 = 1 - 0 = 1$

$s'_0 = 0$ $r_1 = s_1 + \omega^1 s'_1 = 1 + i\cdot 0 = 1$

$s'_1 = 0$ $r_3 = s_1 - \omega^1 s'_1 = 1 - i\cdot 0 = 1$

$\boxed{(1,1,1,1)}$ Of which sequence is $(1,0,0,0)$ is the FFT?

$\boxed{\left(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\right)}$

b) $FFT([1,0,1,-1], i)$ $n=4$ $\boxed{\omega = i}$

$(s_0, s_1) = FFT([1,1], i^2) = FFT([1,1], -1)$

$FFT([1,1], -1)$ $n=2$ $\Rightarrow (2,0)$

$s_0 = FFT(1,1) = 1$ $r_0 = s_0 + \omega^0 s'_0 = 1+1 = 2$

$s'_0 = FFT(1,1) = 1 \quad r_1 = s_0 - \omega^0 s'_0 = 1 - 1 = 0$

$(s'_0, s'_1) = FFT([0,-1], i^2) = FFT([0,-1],-1)$

$FFT([0,-1],-1) \quad n=2 \Rightarrow (-1,1)$

$s_0 = FFT(0,1) = 0 \quad r_0 = s_0 + \omega^0 s'_0 = 0 + (-1) = -1$

$s'_0 = FFT(-1,1) = -1 \quad r_1 = s_0 - \omega^0 s'_0 = 0 - (-1) = 1$

$s_0 = 2 \quad r_0 = s_0 + \omega^0 s'_0 = 2 + (-1) = 1$

$s_1 = 0 \quad r_2 = s_0 - \omega^0 s'_0 = 2 - (-1) = 3$

$s'_0 = -1 \quad r_1 = s_1 + \omega^1 s'_1 = 0 + i \cdot 1 = i$

$s'_1 = 1 \quad r_3 = s_1 - \omega^1 s'_1 = 0 - i \cdot 1 = -i$

$\boxed{(1, i, 3, -i)}$

$\boxed{\text{Sequence of FFT: } \frac{1}{4}(1, -i, 3, i)}$