Carl Cortez
CIS 628
Chapter 6
Lab 7

6.1

As a refresher, symmetric cryptography has the same secret key for encryption and decryption. As talked about in the previous lab, encryption and decryption will appear to be very similar in these circumstances. A key element of Chapter 6 explains that Public-key algorithms are computationally intensive (slow) and are poorly suited for bulk data encryption. Symmetric ciphers are used more frequently because of their speed and capability to encrypt bulk data.

6.2

$rate_{decryptRSA}$ = 100 Kbit/sec = 125,000 bit/sec

$rate_{decryptAES}$ = 17 Mbit/sec = 17(125000) bit/sec

$storage_{DVD}$ = 1 GByte

$Time_{decryptAES} = \frac{1\ GByte}{17\ Mbit}$ seconds

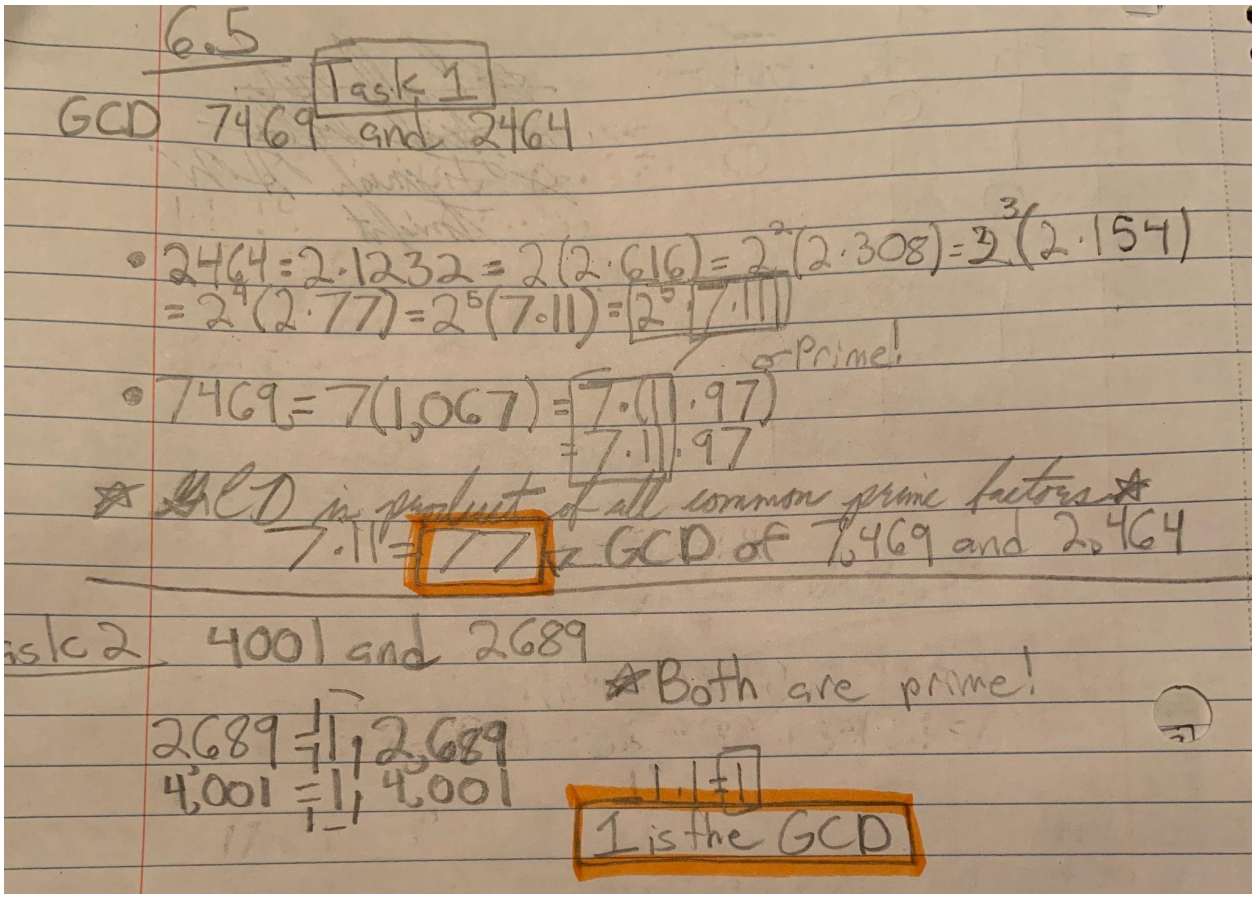
$Time_{decryptRSA} = \frac{1\ GByte}{100\ Kbit}$ seconds

6.3

120 employees at a company with a new security policy need encrypted message exchanges with a symmetric cipher. Number of keys can be found by plugging in for *n* employees using this equation (cc pg. 151):

$\frac{n(n-1)}{2} = \frac{120(120-1)}{2} = \frac{120(119)}{2}$ =60(119)= 7,140 keys.

6.5


6.5
Task 1
GCD 7469 and 2464
• 2464 = 2·1232 = 2(2·616) = 2²(2·308) = 2³(2·154)
= 2⁴(2·77) = 2⁵(7·11) = 2⁵·7·11
• 7469 = 7(1,067) = 7·(11·97)
= 7·11·97
or Prime!
★ GCD is product of all common prime factors ★
7·11 = 77 ← GCD of 7,469 and 2,464
Task 2 4001 and 2689
★ Both are prime!
2689 = 1, 2,689
4,001 = 1, 4,001
1 is the GCD

6.6

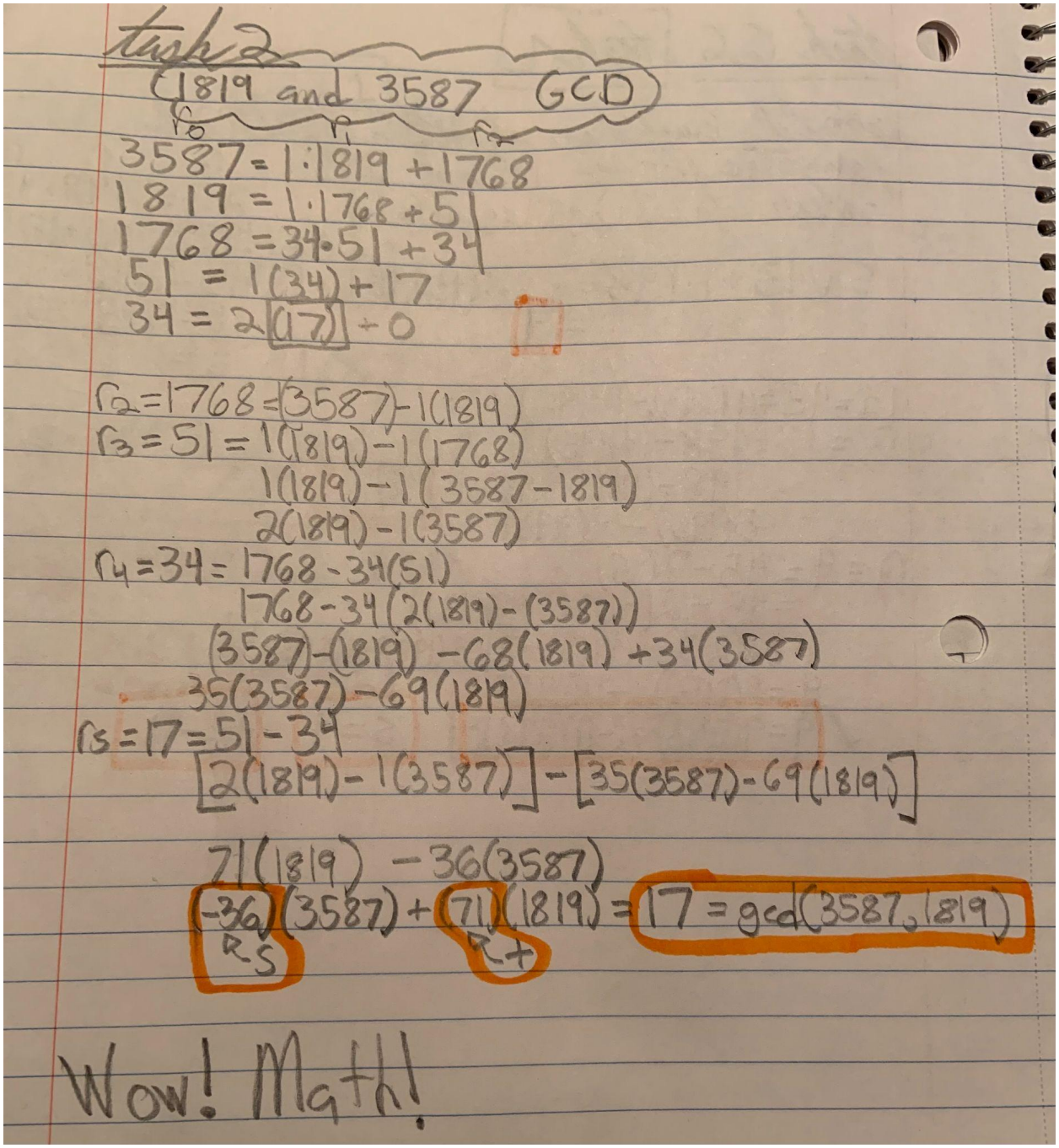
task 6.6 task 1

extended Euclidean algorithm, GCD and parameters s, t, of 198 and 243.
- check if $s \cdot r_0 + t r_1 = \gcd(r_0, r_1)$

r_0 r_1 r_2
$243 = 1 \cdot 198 + 45$
$198 = 4 \cdot 45 + 18$ r_3
$45 = 2 \cdot 18 + 9$
$18 = 2 \boxed{9} + 0$

$s \cdot 243 + t \cdot 198 = \gcd(243, 198)$
$= \boxed{9}$

$r_2 = 45 = (1)(243) - (1)(198)$
$r_3 = 18 = 198 - (4)(45)$
$198 - (4)(1 \cdot 243 - 1 \cdot 198)$
$5(198) - 4(243)$
$r_4 = 9 = 45 - 2(18)$
$= 45 - 2(5(198) - 4(243))$
$= 1(243) - 1(198) - 2[5(198) - 4(243)]$
$9 = 9(243) - 11(198)$
✓ $\boxed{9 = 9(243) + (-11)(198)}$ $\boxed{s = 9}$ $\boxed{t = -11}$


task 2
1819 and 3587 GCD
3587 = 1·1819 + 1768
1819 = 1·1768 + 51
1768 = 34·51 + 34
51 = 1(34) + 17
34 = 2(17) + 0
r2 = 1768 = 3587 - 1(1819)
r3 = 51 = 1(1819) - 1(1768)
1(1819) - 1(3587 - 1819)
2(1819) - 1(3587)
r4 = 34 = 1768 - 34(51)
1768 - 34(2(1819) - (3587))
(3587) - (1819) - 68(1819) + 34(3587)
35(3587) - 69(1819)
r5 = 17 = 51 - 34
[2(1819) - 1(3587)] - [35(3587) - 69(1819)]
71(1819) - 36(3587)
(-36)(3587) + (71)(1819) = 17 = gcd(3587, 1819)
R5
R4
Wow! Math!

6.7

6.7

task 1

inverses of $\mathbb{Z}_m$ with elements a mod m.

a = 7 m = 26 (affine cipher)

$7^{-1} \bmod 26$

$7 = 1 \cdot 7$

$26 = 2 \cdot 13 \cdot 1 \Rightarrow \gcd(7,26) = 1$

$26 = 3 \cdot 7 + 5$
$7 = 1 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 2(1) + 0$

$5 = 26 - 3 \cdot 7$
$2 = 7 - 5$
$7 - (26 - 3 \cdot 7)$
$4(7) - 26$
$1 = 5 - 2(2)$
$5 - 2(4(7) - 26)$
$(26 - 3 \cdot 7) - 8(7) + 2(26)$
$3(26) - 11(7)$
$1 = 3(26) + (-11)(7)$

s = 3
t = -11
gcd(26,7) = 1

$7^{-1} \equiv -11 \bmod 26 \Rightarrow 15$ ★

task 2

19 = a m = 999 $19^{-1} \bmod 999$

$19 = 1 \cdot 19$
$999 = 3^2 \cdot 111 = 3^3 \cdot 37 \cdot 1$ $\Rightarrow \gcd(19,999) = 1$
$999 = 52(19) + 11$
$19 = 1(11) + 8$
$11 = 1(8) + 3$
$8 = 2(3) + 2$
$3 = 1(2) + 1$
$2 = 1(2) + 0$

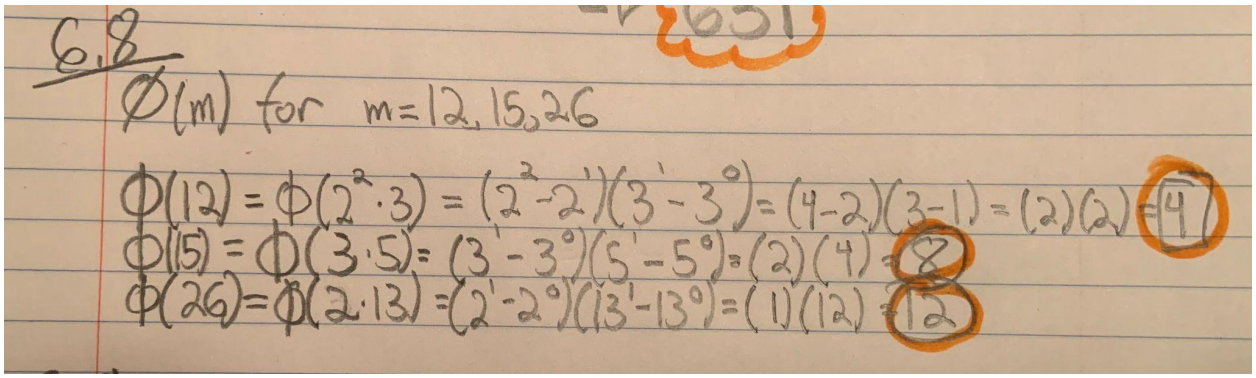
$11 = 999 - 52(19)$
$8 = 19 - 1(11) = 19 - (999 - 52(19))$
$8 = 53(19) - 999$
$3 = 11 - 8 = 11 - (53(19) - 999)$
$999 - 52(19) - (53(19) - 999)$
$3 = 2(999) - 105(19)$

$1 = 3 - 2$
$2 = 8 - 2(3)$
$53(19) - 999 - 2(2(999) - 105(19))$
$2 = 263(19) - 5(999)$

$1 = 2(999) - 105(19) - [263(19) - 5(999)]$
$1 = 7(999) - 368(19)$
$1 = 7(999) + (-368)(19) \Rightarrow 19^{-1} \equiv -368 \bmod 999$

$\Rightarrow 631$

6.8



6.8

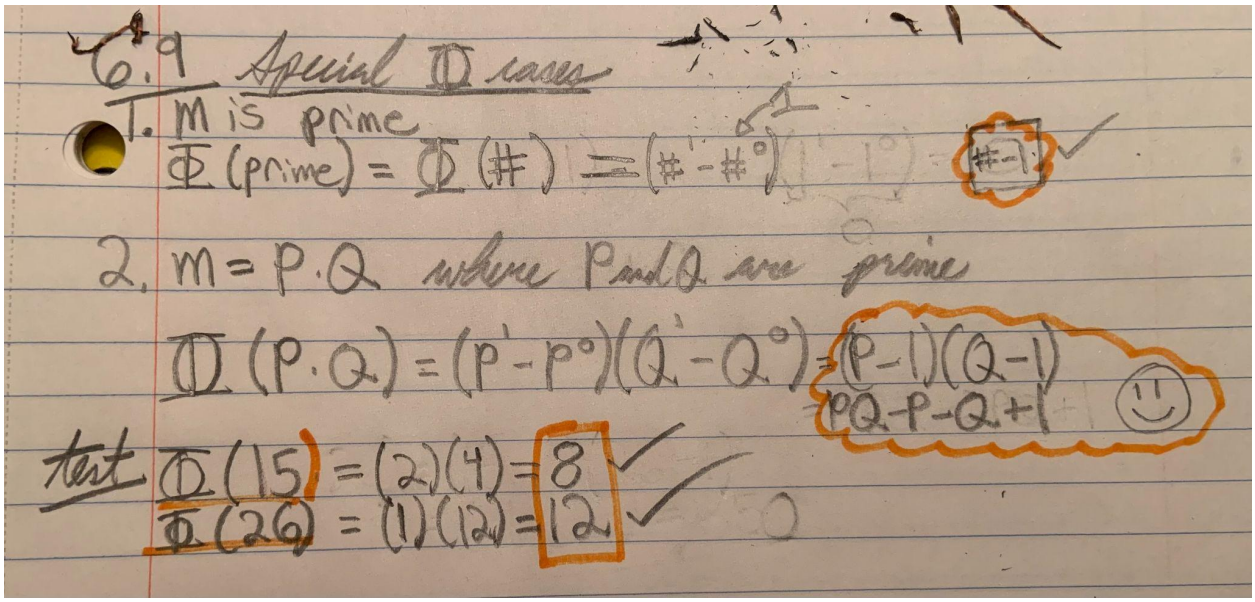
$\phi(m)$ for $m = 12, 15, 26$

$\phi(12) = \phi(2^2 \cdot 3) = (2^2 - 2^1)(3^1 - 3^0) = (4-2)(3-1) = (2)(2) = 4$

$\phi(15) = \phi(3 \cdot 5) = (3^1 - 3^0)(5^1 - 5^0) = (2)(4) = 8$

$\phi(26) = \phi(2 \cdot 13) = (2^1 - 2^0)(13^1 - 13^0) = (1)(12) = 12$

6.9



6.9 Special Φ cases

1. m is prime

$\Phi(\text{prime}) = \Phi(\#) = (\#^1 - \#^0) = \#-1$

2. $m = P \cdot Q$ where P and Q are prime

$\Phi(P \cdot Q) = (P^1 - P^0)(Q^1 - Q^0) = (P-1)(Q-1)$

$= PQ - P - Q + 1$

test $\Phi(15) = (2)(4) = 8$

$\Phi(26) = (1)(12) = 12$