Solutions, Assignment 3

1. $\phi(11413) = 11{,}200$ and $\gcd(7467, 11{,}200) = 1$.

By the Euclidean algorithm we get $3 \cdot 7467 - 2 \cdot 11200 = 1$ so the decryption exponent is 3.

The original plaintext was $5859^3 \equiv 1415 \mod 11413$ so was 1415.

6. Bob should compute b_1 s.t. $bb_1 \equiv 1 \mod \phi(n)$. and compute $e^{b_1} \mod n$ to obtain the original message. To see that this works, note that

$$e \equiv \left((m^a)^b\right)^{a_1} \equiv \left(m^{aa_1}\right)^b \equiv m^b \mod n$$

and so $e^{bb_1} \equiv m^{bb_1} \equiv m \mod n$.

8. This does not increase the security because it is equivalent to using e, e_2 (or $e, e_2 \mod \phi(n)$) which in general is of the same order of security.

12. We have $(516107 \times 187722)^2 \equiv 14^2 \mod n$.
and $516107 \times 187722 \equiv 289038 \mod n$.

So $289038^2 \equiv 14^2 \mod n$ and $289038 \not\equiv \pm 14 \mod n$

So $\gcd(289038 - 14, 642401) = 1129$ and

$642401 = 1129 \times 569$.

15 a) If n is odd then $\gcd(2, n) = 1$. If n is prime then

$$2^{n-1} \equiv 1 \bmod n. \quad \text{by Fermat.}$$

Hence if $k \equiv 2^{\frac{n-1}{2}} \bmod n$, $k \not\equiv \pm 1 \bmod n$ and $k^2 \not\equiv 1 \bmod n$ then $2^{n-1} \not\equiv 1 \bmod n$ so n is <u>not</u> prime.

b) If $k^2 \equiv 1 \bmod n$ and $k \not\equiv \pm 1 \bmod n$ then $\gcd(k+1, n) \neq 1, n$ and so gives a non-trivial factor of n by the Basic Principle.

20. Choose d s.t. $ed \equiv 1 \bmod (p-1)(q-1)(r-1)$ since $\phi(n) = (p-1)(q-1)(r-1)$.

If we encode a message m be $c = m^e \bmod n$ then if $\gcd(m, n) = 1$ we get $c^d \equiv m \bmod n$.

If the $\gcd(m, n) \neq 1$ then we may assume it is p or pq. If $\gcd(m, n) = p$ then

$m^{ed} \equiv m \bmod p$ and $m^{ed} \equiv m \bmod qr$ by Euler. So $m^{ed} \equiv m \bmod pqr$ by the Chinese Remainder Theorem.

If $\gcd(m, n) = pq$ then $m^{ed} \equiv m \bmod pq$ and $m^{ed} \equiv m \bmod r$ by Fermat and again we are done by the CRT.