CPSC 353 Project 2 Katie Stevens

1. You would have to use a cipher-text only attack to decrypt the message.

2. The key exchange problem happens when a third party intercepts and exchange of a secrect symmetric-key so their communication channel becomes unsecure.

3. If there is no public key infrastructure, there is the problem of not being able to verify the identity of the owner of the key, you don't know if the message or the public key has been tampered with.

4. AVFFDDD ADVAXGF FXVXVGX

C	E	N	P	R	T	Y
A	F	D	V	G	X	V
V	D	A	A	F	V	G
F	D	D	X	F	X	X

⇒

E	N	C	R	Y	P	T
F	D	A	G	V	V	X
D	A	V	F	G	A	V
D	D	F	F	X	X	X

Not used

F	A	V	X	A	F	A	D	F	row
D	G	V	D	V	G	V	D	F	column
I	A	M	N	O	B	O	D	Y	using ADFGVX array

5. Division Algorithm Theorem

Given integers a,b with $b > 0$ ∃ unique integers q, r satisfying

$a = qb + r \quad 0 \leq r \leq b$

Where

q is the quotient

b is the divisor

r is the remainder

6. Let $a = 3q$

$(3q)^3 = 27q^3 = 9(3q^3)$

$\boxed{= 9k}$

$(3q+1)^3 = (3q+1)(9q^2+6q+1)$

$= 27q^3 + 27q^2 + 9q + 1$

$= 9(3q^3 + 3q^2 + q) + 1$

$\boxed{= 9k + 1}$

$(3q+2)^3 = (3q+2)(9q^2 + 12q + 4)$

$= (27q^3 + 36q^2 + 12q + 18q^2 + 24q + 8)$

$= 27q^3 + 54q^2 + 36q + 8$

$= 9(3q^3 + 6q^2 + 4q) + 8$

$\boxed{= 9k + 8}$

7. Let $a = 3q$

$a = 3q$ $\quad (3q)^2 = 9q^2$

$= 3(3q^2)$

$\boxed{= 3k}$

$a = 3q + 1$ $\quad (3q+1)^2 = 9q^2 + 6q + 1$

$= 3(3q^2 + 2q) + 1$

$\boxed{= 3k + 1}$

8. $3a^2 - 1$

$3(a^2) - 1$

$3k - 1$

Not a perfect square

9. $a = 482 \quad b = 1180$

$$\begin{array}{r} 2 \\ 482\,\overline{)\,1180} \\ -964 \\ \hline 216 \end{array}$$

$1180 = 482 \cdot 2 + 216$

$482 = 216 \cdot 2 + 50$

$216 = 50 \cdot 4 + 16$

$50 = 16 \cdot 3 + 2$

$16 = 2 \cdot 8 + 0$

$\boxed{\gcd(482, 1180) = 2}$

10. $482S + 1180T = \gcd(482, 1180)$

$482S + 1180T = 2$

$2 = 50 - 16(3)$

$16 = 216 - 50(4)$

$2 = 50 - (3)(216 - 50(4))$

$= (-3)216 + (13)\,50 \qquad 50 = 482 - 216(2)$

$= (-3)216 + 13(482 - 216(2))$

$= (-29)216 + 13(482) \qquad 216 = 1180 - 482(2)$

$= 13(482) + (-29)(1180 - 482(2))$

$= (71)482 + (-29)1180$

$\boxed{S = 71 \quad T = -29}$