Tutorial -6

SOEN-321

Problem-1

Let x=111 and y=19301.   Factor n=21311 using the fact that $x^2 \equiv y^2 \; mod \; n$.

$x^2 - y^2 = 0 \; mod \; n$

$x^2 - y^2 = Kn$

$(x + y)(x - y) = k_1 k_2 n$

$(x + y)(x - y) = k_1 p k_2 q$

$\gcd(x \pm y, n) = p \; or \; q$

$\gcd(111 + 19301, 21311)$

$\gcd(19412, 21311)$

$21311 = 19412 + 1899$

$19412 = 10 \times 1899 + 422$

$1899 = 4 \times 422 + 211$

$422 = 2 \times 211 + 0$

$\gcd(19412, 21311) = p = 211$

$q = \frac{n}{p} = \frac{21311}{211} = 101$

Problem 2

Suppose Bob has an RSA Cryptosystem with a large modulus n for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (i.e., A<->0, B<->1, etc.), and then encrypting each residue modulo n as a separate plaintext character.

Describe how Eve can easily decrypt a message which is encrypted in this way.

Eve can construct a lookup table for all the valid 26 ciphertexts by encrypting the letters A to Z using Bob's public key.

Then Eve can use this table (or more precisely the inverse of this table) to decrypt any ciphertext encrypted by Alice

m	$c = m^e \bmod n$
$A = 0$	$c = 0$
$B = 1$	$c = 1$
…	…
$Z = 25$	…