SOEN 321

Prob. 1 Let x=111 and y=19301. Factor n=21311 using the fact that $x^2 \equiv y^2$ mod n.

Ans.
Note that
$x^2=y^2$ mod n -> x^2-y^2 =0 mod n -> (x-y)(x+y)=0 mod n ->
(x-y)(x+y)=Kn=Kpq for some integer K). Let K=k1 K2. Thus we have
(x-y)=k1 p & x-y)=k2 q
Then we can factor n as follows:
gcd(x ±y,n)=p or q.

Prob. 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 Ever can easily decrypt a message which is encrypted in this way.

Ans. 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) tp decrypt any ciphertext encrypted by Alice.

Prob. 3 . Determine the problems in the following protocol in which A wants to establish a shared session key with B using the help of a trusted authority S

A→S: A, B
S→A: K_{AB}
A→B: A, K_{AB}

Ans. The key is sent in the clear.

Prob. 4 Consider the following authentication protocol

A → B: T_A, $Sig_A(T_A,B)$

(i) What is the objective of the time stamp T_A?

(ii) After this protocols is executed
(a) B is authenticated to A
(b) A is authenticated to B
(c) Both A and B are authenticated to each other
Ans. The time stamp ensures the freshness of the signature and prevents replay attacks. "A" is authenticated to B.