

SOEN 321

(Although these questions will be solved with you during the tutorial, you should try solving them by yourself before the tutorial)

Prob. 1 Consider an RSA system with $p=17$, $q=11$ and $e=3$.

- Find m corresponding to $c=156$
- Repeat part (a) above using the Chinese remainder theorem

Ans.

$$d=e^{-1} \bmod 160=107$$

$$mp=c^d \bmod p=7$$

$$mq=c^d \bmod q=7$$

Using CRT we get $m=7$ (note that this is just a coincidence and in general we can get different values for mp, mq and m)

Problem 2.

Consider an RSA system with $n=899$. If the attacker knows that the system was (poorly) constructed using twin primes (i.e., p and q are twin primes). Show how that attacker can break this system.

Ans. $p(p+2)=n \rightarrow p^2+2p+n=0$. Solve 2nd order equation in p to get $p=29$ and $q=31$.

Prob 3.

Consider an RSA system with $n=21311$. Show how the attacker can factor n if she knows that $\phi(n)=21000$.

Ans. $\phi(n)=(p-1)(n/p-1)$

Thus we can form a quadratic equation in p . Solving for p we get $p=101$ or 211 .

Prob 4. Consider an RSA system with $n=143$, $e_1=7$ and $e_2=17$. Suppose the same message m was sent to the two users above and the attacker observed the ciphertext $c_1=42$ and $c_2=9$. Show how the attacker can recover the message.

Ans.

Use Extended Euclidian algorithm to find a and b such that

$$a e_1 + b e_2 = 1$$

Then we obtain m as $c_1^a * c_2^b \bmod n$

$$m=3$$