Tutorial 4

SOEN-321

Exercise 2-2

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.

$n = 899$

Twin primes => $q = p + 2$

$n = pq = p(p + 2) = p^2 + 2p$
$p^2 + 2p - n = 0$
$p^2 + 2p - 899 = 0$

$p = 29$
$q = 29 + 2 = 31$

$$p = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$p = \frac{-2 \pm \sqrt{2^2 - 4 \times -899}}{2}$$

$$p = \frac{-2 \pm 60}{2}$$

$p = 29$ *or* ~~$p = -31$~~

Exercise 2-3

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

$n = pq \qquad q = \frac{n}{p}$

$\phi(n) = (p-1)(q-1) = (p-1)\left(\frac{n}{p} - 1\right)$

$\phi(n) = n - p - \frac{n}{p} + 1$ -Multiply by p

$p\phi(n) = np - p^2 - n + p$ -Subtract pΦ(n)

$np - p^2 - n + p - p\phi(n) = 0$

$p^2 - np - p + p\phi(n) + n = 0$

$p^2 + (\phi(n) - n - 1)p + n = 0$

$p^2 + (21000 - 21311 - 1)p + 21311 = 0$

$p^2 - 312p + 21311 = 0$

$p = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

$p = \frac{312 \pm \sqrt{312^2 - 4 \times 21311}}{2}$

$p = \frac{312 \pm 110}{2}$

$p = 211 \; or \; p = 101$

Exercise 2-4

Consider an RSA system with n=143, e1=7 and e2=17. Suppose the same message m was sent to the two users above and the attacker observed the ciphertext c1=42 and c2=9. Show how the attacker can recover the message.

Common modulus attack (Set 3 – Slide 24)

Use extended Euclidean algorithm to find a, b such that

$ae_1 + be_2 = 1$

$egcd(17, 7)$

$17 = 2 \times 7 + 3$

$7 = 2 \times 3 + 1$

$1 = 7 - 2 \times 3$

$1 = 7 - 2 \times (17 - 2 \times 7)$

$1 = 5 \times 7 - 2 \times 17$

$a = 5, b = -2$

$m = c_1^a \, c_2^b \, mod \, n$

$m = 42^5 \times 9^{-2} \, mod \, 143$

$42^5 \, mod \, 143 = 100$

$9^{-2} \, mod \, 143 = 16^2 \, mod \, 143 = 113$

$m = 100 \times 113 \, mod \, 143 = 25600 \, mod \, 143$

$m = 3$

*Calculation steps for inverse in next slide

Exercise 2-4 – Calculation steps

$9^{-2}\ mod\ 143 = (9^{-1})^2\ mod\ 143$

$\underline{9^{-1}\ mod\ 143}$
$143 = 15 \times 9 + 8$
$9 = 1 \times 8 + 1$

$1 = 9 - 1 \times 8$
$1 = 9 - 1 \times (143 - 15 \times 9) = 16 \times 9 - 143\ mod\ 143$
$1 = 16 \times 9\ mod\ 143$