암호학기초 HW#5 20191629 이무현

Chapten 10

12. In RSA...

a. Given $n = 221$, $e = 5$, find d.

$221 = p \cdot q \Rightarrow p = 13,\ q = 17.$

$\phi(n) = \phi(221) = 192,\ d = e^{-1} \bmod \phi(n) = 5^{-1} \bmod 192$

$\Rightarrow d = 77.$

b. Given $n = 3937$, $e = 17$, find d.

$3937 = p \cdot q \Rightarrow p = 31,\ q = 127.$

$\phi(n) = \phi(31 \times 127) = 3780,\ d = e^{-1} \bmod \phi(n) = 17^{-1} \bmod 3780.$

$\Rightarrow d = 3113.$

c. Given $p = 19$, $q = 23$, $e = 3$, find n, $\phi(n)$, d.

$n = p \cdot q = 19 \times 23 = 437.$

$\varphi(n) = \varphi(19 \times 23) = 396.$

Here, $\gcd(\varphi(n), e) = \gcd(396, 3) \neq 1.$

Thus, no such d exists.

13. To understand RSA, find d if you know $e = 17$, $n = 187$.

$n = p \times q \Rightarrow 187 = 17 \times 11 \Rightarrow p = 17,\ q = 11.$

$\varphi(n) = \varphi(17 \times 11) = 160.;\quad d = e^{-1} \bmod \varphi(n) = 17^{-1} \bmod 160.$

$\Rightarrow d = 113.$

It is fairly easy to find d in this example, as n is small and its factors are trivial. n and $\varphi(n)$ must be sufficiently large in order to make RSA secure.

14. In RSA, given n and $\varphi(n)$, calculate p and q.

Here, $n = p \cdot q$ by definition. Thus, $\varphi(n) = (p-1)(q-1).$

$$\left.\begin{aligned} n &= p \cdot q. \\ \varphi(n) &= p \cdot q - p - q + 1. \end{aligned}\right] \rightarrow n - \varphi(n) + 1 = pq - (pq - p - q + 1) + 1 = p + q.$$

We can isolate p and q where $D = n - \varphi(n) + 1$, since

$$x^2 - (p+q)x + pq = \emptyset,\quad \left.\begin{aligned} p &= \frac{(p+q) + \sqrt{(p+q)^2 - 4pq}}{2} = \frac{D + \sqrt{D^2 - 4n}}{2} \\ q &= \frac{(p+q) - \sqrt{(p+q)^2 - 4pq}}{2} = \frac{D - \sqrt{D^2 - 4n}}{2}. \end{aligned}\right\}\text{answer}$$

암호학기초 HW#5

20191629 이주현

15. In RSA, given $e=13$, $n=100$. Encrypt the message "HOW ARE YOU".

RSA encryption function is : $c = m^e \bmod n$.

H O W . A R E Y O U

07 14 22 26 00 17 04 26 24 14 20

07 44 52 76 00 37 64 76 24 44 00

The encrypted message cannot be decrypted because n cannot be decomposed into two primes, p and q.

19. Show how Eve can use the chosen-ciphertext attack.

i) Eve finds a number in $\mathbb{Z}_{143}^*$. Let's say she found 17.

ii) Eve chooses a ciphertext $57 \times 17^7 \bmod 143 = 137$.

iii) Eve accesses Bob's computer and decrypts 137. It's 136.

iv) Eve calculates $136 \times 17^{-1} \bmod 143$. It is 8, the plaintext of the intercepted Ciphertext.

22. Using the Rabin cryptosystem w/ $p=47$, $q=11$.

a. $n = 47 \times 11 = 517$. $\Rightarrow$ $C = p^2 \bmod 517 = 17^2 \bmod 517 = 289$.

b. Four candidates:

$a = C^{(P+1)/4} \bmod p = 289^{12} \bmod 47 \Rightarrow a = \pm 17$.

$b = C^{(q+1)/4} \bmod q = 289^3 \bmod 11. \Rightarrow b = \pm 5$.

$$\left.\begin{array}{l} 1)\ P_1 \equiv 17 \bmod 47 \text{ and } 5 \bmod 11. \rightarrow 346. \\ 2)\ P_2 = 17 \bmod 47 \text{ and } -5 \bmod 11 \rightarrow 17.\checkmark \\ 3)\ P_3 = -17 \bmod 47 \text{ and } -5 \bmod 11 \rightarrow 171 \\ 4)\ P_4 = -17 \bmod 47 \text{ and } 5 \bmod 11 \Rightarrow 500. \end{array}\right\} \text{possible plaintexts.}$$

24. Since the order of transmission is significant as:

$C_2 \times (C_1^d)^{-1} \neq C_1 (C_2^d)^{-1}$

The receiver cannot correctly decrypt the ciphertext should two values are swapped.

25. Show how Eve can use a known-plaintext attack.

i) Assuming $p=53$ and $d=3$, the intercepted ciphertexts are:

$C_1 = 35$, $C_2 = 19$, $C_1' = 35$, $C_2' = 32$.

ii) Eve intercepts the message.

$P' = C_2' \times (e_2^r)^{-1} \bmod p = C_2' \times (C_2 \times p^{-1})^{-1} \bmod p = C_2' \times C_2^{-1} \times p \bmod p$.

$\Rightarrow 32 \times 19^{-1} \times 17 \bmod 53 = 7616 \bmod 53 = \boxed{37}$.