CSS322 – Public Key Cryptography Notes

RSA Key Generation

$p = 17 \qquad q = 11$

$$
\begin{aligned}
n &= p \times q \\
&= 17 \times 11 \qquad \phi(p) = p-1 \\
&= 187
\end{aligned}
$$

$$
\begin{aligned}
\phi(187) &= \phi(17 \times 11) \\
&= \phi(17) \times \phi(11) \\
&= 16 \times 10 \\
&= 160
\end{aligned}
$$

$\gcd(e, 160) = 1 \qquad 1 < e < 160$

$\cancel{2}\ 3\ \cancel{4}\ \cancel{5}\ \cancel{6}\ 7\ 9\ 11 \ldots$

$e = 7$

$7 \times d \bmod 160 = 1$

$7 \times d = 161 \qquad d = 23$

$PU_B = (e = 7, n = 187)$

$PR_B = (d = 23, n = 187)$

Figure 1: RSA Key Generation; Lecture 10

$$A \xrightarrow{C=11} B$$

$M = 88$

$C = 88^7 \bmod 187$
$= 11$

$M' = 11^{23} \bmod 187$
$= 88$ ✓

Figure 2: RSA Encryption and Decryption; Lecture 10

$$C = M^e \bmod n \quad M = C^d \bmod n$$

$$M' = C^d \bmod n$$
$$= (M^e \bmod n)^d \bmod n$$
$$= (M^{ed} \bmod n) \bmod n$$
$$M' = M^{ed} \bmod n$$

$$a = a^{ed} \bmod n$$
$$a = a^{\phi(n)+1} \bmod n$$

$$ed = \phi(n) + 1 \qquad 21 = 20 + 1$$

$$e \times d \bmod \phi(n) = 1 \qquad 21 \bmod 20 = 1$$

$$e : \ RP(e, \phi(n)) \Rightarrow \gcd(e, \phi(n)) = 1$$

Calculate d

Figure 3: Why RSA Successfully Decrypts; Lecture 11

$$A \xrightarrow{C=11} B$$

Attacker

Know: $C = 11$, $PU_B = (e = 7, n = 187)$

$$m = C^{d} \bmod n$$

$$ed \bmod (\phi(n)) = 1$$

$$7 \times d \bmod (\phi(187)) = 1$$

$\phi(187)$: Factor 187 into primes

$RP(1,187)$, $RP(2,187)$ .... $RP(186,187)$

Figure 4: RSA Attack: Find totient; Lecture 11

Knows: $C = 11$, $e = 7$, $n = 187$

$(m_1 = 17, C_1 = 85)$

Find d ??

$$m = C^{d} \bmod n$$

$$d = \mathrm{dlog}_{c,n}(m)$$

Figure 5: RSA Attack: Find Discrete Log; Lecture 11

$$PU = (e = 7,\ n = 299)$$
$$PR = (d = \quad,\ n = 299)$$
$$ed \equiv 1 \pmod{\phi(n)}$$
$$7d \bmod \phi(299) = 1$$

$$n = pq \qquad\qquad n = 299$$
$$= pq$$
$$p = 13$$
$$q = 23$$
$$\phi(n) = \phi(pq)$$
$$= \phi(p)\phi(q)$$
$$= (p-1)(q-1)$$
$$\phi(299) = 12 \times 22$$
$$= 264$$

$$7 \times \_\_ \bmod 264 = 1$$
$$7 \times \_\_ = 265 \quad \times$$
$$7 \times \_\_ = (264 \times 2) + 1 \quad \times$$
$$7 \times \underline{151} = (264 \times 4) + 1 \quad \checkmark$$
$$d \ \checkmark$$

Figure 6: Example of Breaking RSA Key Pair; Lecture 12