CSCI 8920 Homework Week 13 Derivations

Susannah Go

1

Let c, d, e, m, and n denote the usual values for the RSA algorithm so that $c = m^e \mod n$ and $m = c^d \mod n$. Let r be any random value such that $\gcd(r, n) = 1$. Now, given ciphertext c create a masked version $c_* = cr^e$. Let m_* be the decryption of c_*. The following calculations show how to recover m:

$$\begin{aligned}
m_* &= c_*^d \mod n \\
&= (cr^e)^d \mod n \\
&= (m^e r^e)^d \mod n \\
&= (mr)^{ed} \mod n \\
&= (mr)^{k\phi(n)+1} \mod n \quad (\text{for some } k \in \mathbb{Z} \text{ since } ed \equiv 1 \mod \phi(n)) \\
&= (mr)^{k\phi(n)}(mr) \mod n \\
&= \left(((mr)^{\phi(n)} \mod n)^k\right)(mr \mod n) \\
&= 1^k \cdot mr \mod n \quad (\text{Euler's Theorem}) \\
&= mr \mod n
\end{aligned}$$

Thus $m = m_* r^{-1} \mod n$.

2

Suppose we know two public keys (n, e_1) and (n, e_2). We know that message m has been encrypted with both keys, giving $c_1 = m^{e_1} \mod n$ and $c_2 = m^{e_2} \mod n$. We known that $\{e_1, e_2\} = \{3, 2^{16} + 1\}$, so e_1 and e_2 are co-prime. Thus $e_1 = ke_2 - 1$ for some (easily computable) integer k. The following is a derivation showing how to recover m:

$$\begin{aligned}
c_1 &= m^{e_1} \mod n \\
&= m^{ke_2 - 1} \mod n \\
&= m^{ke_2} \cdot m^{-1} \mod n \\
&= (m^{e_2})^k \cdot m^{-1} \mod n \\
&= (m^{e_2})^k \cdot m^{-1} \mod n \\
&= c_2^k \cdot m^{-1} \mod n
\end{aligned}$$

Multiply on both sides by m and then c_1^{-1} to get $m = c_1^{-1} c_2^k$.