Assignment 5 (CSE-4137)

Raheeb Hassan (Roll: AE-42)

March 29, 2022

Answer to Problem 1

We know that, due to how the RSA algorithm is designed

$$e_b \cdot d_b \equiv 1 \mod \phi(n)$$

By definition of the modulo operator

$$e_b \cdot d_b = 1 + \phi(n) \cdot k$$
$$\phi(n) \cdot k = e_b \cdot d_b - 1$$

So, the required multiple of $\phi(n)$ is $V = e_b \cdot d_b - 1$

Answer to Problem 2

As e_a is relatively prime to V, using extended euclidean algorithm we can find d such that,

$$d \cdot e_a = 1 \mod V$$

That is, we find the inverse of e_a modulo V.
Now, by definition of the modulo operator

$$\begin{aligned}
&d \cdot e_a = 1 + V \cdot k' \\
&d \cdot e_a = 1 + (\phi(n) \cdot k) \cdot k' \\
&d \cdot e_a = 1 + \phi(n) \cdot k'' \\
&m^{d \cdot e_a} = m^{1+\phi(n) \cdot k''} && (m \in Z_n) \\
&m^{d \cdot e_a} = m \cdot \left(x^{\phi(n)}\right)^{k''} \\
&m^{d \cdot e_a} = m && (\text{Euler's theorem, } m^{\phi(n)} = 1)
\end{aligned}$$

Therefore, if we encrypt any message m with secret key d, it can be decrypted using e_a.

$$c^{e_a} = (m^d)^{e_a} = m^{d \cdot e_a} = m$$

In other words, Bob can invert Alice's trapdoor permutation and obtain her signature on m (by signing it with d)

$$\sigma_a = H(m)^d$$

Answer to Problem 3

If e_a is not relatively prime to V, then $gcd(e_a, V) \neq 1$. Let the prime factorization of V be:

$$V = \prod {p_i}^{q_i}$$

Now, we define,

$$W = \prod {p_i}^{q_i} \text{ where } p_i | e_a$$
$$V' = V/W$$

As W contains all the multiples of the common factors of V and e_a, $gcd(e_a, V') = 1$.
Moreover, as e_a and $\phi(n)$ have no common factors, we can be sure that V' is also a multiple of $\phi(n)$.

Now, we can use V' instead of V and use the same procedure as problem 2.