Prob 41

$$C_2 = ((S^E \bmod N)\, C) \bmod N$$

$$P_2 = C_2^D \bmod N$$

$$P \overset{?}{=} P_2 S^{-1} \bmod N$$

$$P \overset{?}{\equiv} P_2 S^{-1} \pmod N$$

$$P S S^{-1} \overset{?}{\equiv} P_2 S^{-1} \pmod N$$

$$\overset{?}{\equiv} \{[((S^E \bmod N)\, C) \bmod N]^D \bmod N\}\, S^{-1} \pmod N$$

$$P S \overset{?}{\equiv} \{[((S^E \bmod N)\, C) \bmod N]^D \bmod N \pmod N$$

$$\overset{?}{\equiv} ((S^E \bmod N)\, C)^D \bmod N \pmod N$$

$$\overset{?}{\equiv} ((S^E \bmod N)^D\, C^D) \bmod N \pmod N$$

$$\overset{?}{\equiv} \{[\underbrace{(\underbrace{S^E \bmod N}_{S \text{ encrypted}})^D \bmod N}_{S \text{ decrypted}}]\,[\underbrace{C^D \bmod N}_{P}]\} \bmod N \pmod N$$

$$\overset{?}{\equiv} \{S P\} \bmod N \pmod N$$

$$P S \overset{\checkmark}{\equiv} P S \pmod N$$

$$P = \underbrace{P \bmod N = C^D \bmod N}_{P \equiv C \pmod N}$$

$$S S^{-1} \bmod N = 1 \implies S S^{-1} \equiv 1 \pmod N$$

$$xN + 1 = S S^{-1}$$

$$y(xN + 1) = y S S^{-1}$$

$$y x N + y = y S S^{-1} \implies y S S^{-1} \equiv y \pmod N$$