Seth Landis

Diffie-Hellman key exchange

5. Common prime $n=11$ User A: pub $Y_a = 9$
Primitive root $g=2$ User B: pub $Y_b = 3$

a) What is A's private key?

$Y_a = g^{x_a} \bmod n$

$9 = 2^{x_a} \bmod 11$

1	2	3	4	5	6	7	8
2	4	8	16	32	64	128	256
2	4	8	5	10	9	7	3

$x_a = 6$

b) B's private key $3 = 2^{X_b} \bmod 11$ $X_b = 8$

$X = 2^6 \bmod 11$ $Y = 2^8 \bmod 11$
$9 = 64 \bmod 11$ $3 = 256 \bmod 11$

$3^6 \bmod 11$ $9^8 \bmod 11$

$3 = 3$

$\boxed{K=3}$

RSA

Seth Luders

$P^e \bmod n$ = encrypt $(P^e)^d \bmod n = P$

b)

Ciphertext $C = 10$

User's public key is $e = 5$, $n = 35$

$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$

$\varphi(n) = (5-1)(7-1)$

$= 4 \cdot 6$

$= 24$

$e = 2 \Rightarrow \gcd(e, 24) = 2$

$e = 3 \Rightarrow \gcd(e, 24) = 3$

$e = 4 \quad = 4$

$e = 5 \Rightarrow \gcd(e, 24) = 1$ ✓

$d * e \bmod \varphi(n) = 1$

$d = (1 + k * \varphi(n))/e$

$d = (1 + k \cdot 24)/5$

$k = 0 = 1/5$

$k = 1 = 5$ ✓

$d = 5$.

Reminder: $C = 10$, $e = 5$, $n = 35$

$P = C^d \bmod n$

$P = 10^5 \bmod 35$

$P = 100000 \bmod 35$

$P = 5$

$$\begin{array}{r|l} & 2857 \quad r5 \\ \hline 35 & 100000 \\ & 70 \\ \hline & 300 \\ & 280 \\ \hline & 200 \\ & 175 \\ & 250 \end{array}$$

$$\begin{array}{r|l} & 4 \\ 35 & \\ 8 & \\ \hline 40 & \\ 240 & \\ 280 & \end{array} \qquad \begin{array}{r|l} 35 & \\ 7 & \\ \hline 35 & \\ 210 & \\ 245 & \end{array}$$