

# Diffie Hellman Key Exchange

	Alice	Evil Eve	Bob
	Alice and Bob exchange a Prime (P) and a Generator (G) in clear text, such that $P > G$ and G is Primitive Root of P $G = 7, P = 11$	Evil Eve sees $G = 7, P = 11$	Alice and Bob exchange a Prime (P) and a Generator (G) in clear text, such that $P > G$ and G is Primitive Root of P $G = 7, P = 11$
Step 1	Alice generates a random number: $X_A$ $X_A = 6$ (Secret)		Bob generates a random number: $X_B$ $X_B = 9$ (Secret)
Step 2	$Y_A = G^{X_A} \pmod{P}$ $Y_A = 7^6 \pmod{11}$ $Y_A = 4$		$Y_B = G^{X_B} \pmod{P}$ $Y_B = 7^9 \pmod{11}$ $Y_B = 8$
Step 3	Alice receives $Y_B = 8$ in clear-text	Evil Eve sees $Y_A = 4, Y_B = 8$	Bob receives $Y_A = 4$ in clear-text
Step 4	Secret Key $= Y_B^{X_A} \pmod{P}$ Secret Key $= 8^6 \pmod{11}$ 🔑 Secret Key = 3		Secret Key $= Y_A^{X_B} \pmod{P}$ Secret Key $= 4^9 \pmod{11}$ 🔑 Secret Key = 3

- **Diffie–Hellman key exchange (D–H)** is a specific method of exchanging keys
- Earliest practical examples of key exchange implemented within the field of cryptography
- Exchange allows two parties having no prior knowledge to jointly establish a shared secret key
- This key can then be used to encrypt subsequent communications