1 Diffie-Hellman

- Elegir un Primo p y una base g, donde $\langle g \rangle$ genera $\mathbb{Z}_p^*$ (orden de g mod p debe ser $p-1$)
- Claves privadas a y b donde $1 < a, b < p$.
- Publicas: $A = g^a \bmod p$, $B = g^b \bmod p$
- Secreto compartido: $S_A = B^a = S_B = A^b$

2 RSA

- Elegir primos p y q. Calcular $n = pq$, $\phi(n) = (p-1)(q-1)$
- Escoger exponente publico e con $1 < e < \phi(n)$, $\gcd(e, \phi(n)) = 1$
- Calcular $d = e^{-1} \bmod \phi(n) \implies d \cdot e \equiv 1 \bmod \phi(n)$. Buscar la forma: $e \cdot x + \phi(n) \cdot y = 1$
  Llave publica $= (n, e)$
  Llave privada $= (n, d)$.
- Cifrado de mensajes: $C = m^e \bmod n$. Se envia (n, C)
- Descifrado de mensaje: $\hat{m} = C^d \bmod n$, Comprobar: $\hat{m} = m$
- **Cifrado de firmas:** $h = hash(m)$, Firma $s = h^d \bmod n$. Se envía (m, s)
- **Verificación de firma:** $\hat{h} = s^e \bmod n$, Comprobar: $\hat{h} = h$

3 ElGamal

- Elegir un primo p y una base g, donde $\langle g \rangle$ genera $\mathbb{Z}_p^*$ (orden de g mod p debe ser $p-1$)
- Clave privada x, publica $y = g^x \bmod p$
- Mensaje m y valor aleatorio k
- Par cifrado (c_1, c_2): $c_1 = g^k \bmod p$, $c_2 = m \cdot y^k \bmod p$
- Desencriptar mensaje: Calcular $s = (c_1)^x \bmod p$, despues calcular $s^{-1} \bmod p$, finalmente $\hat{m} = c_2 \cdot s^{-1} \bmod p$. Comprobar: $\hat{m} = m$