ECIES Encryption

From the Ethereum project website.[1]

> Alice wants to send an encrypted message that can be decrypted by Bob's static private key k_B. Alice knows about Bob's static public key K_B.
>
> To encrypt the message m, Alice generates a random number r and corresponding elliptic curve public key $R = r * G$ and computes the shared secret $S = P_x$ where $(P_x, P_y) = r * K_B$. She derives key material for encryption and authentication as $k_E \,\|\, k_M = \mathtt{KDF}(S, 32)$ as well as a random initialization vector `iv`. Alice sends the encrypted message $R \,\|\, \mathtt{iv} \,\|\, c \,\|\, d$ where $c = \mathtt{AES}(k_E, \mathtt{iv}, m)$ and $d = \mathtt{MAC}\big(\mathtt{sha256}(k_M), \mathtt{iv} \,\|\, c\big)$ to Bob.

[1] https://github.com/ethereum/devp2p/blob/master/rlpx.md