Common Asymmetric Ciphers

The following table describes some of the more common asymmetric ciphers. Of course, many other ciphers exist, and more are being developed all the time.

Cipher	Description
Diffie-Hellman	This cipher is one of the oldest public key ciphers, and it is credited to Whitfield Diffie and Martin Hellman. Through a series of mathematical steps, the sender and receiver calculate the same shared secret key, using undisclosed private keys. Certain starting values for the calculations are set long before communication begins. Then, new private values are chosen to calculate the session key. The session key is discarded at the end of the session. (A new key is chosen for each communication session.) Diffie-Hellman is vulnerable to man-in-the-middle attacks. In this attack, Eve may intercept communications between Alice and Bob, calculating separate session keys with each. To Alice and Bob, it would not be clear that Eve was operating between them.
RSA	RSA is one of the most well-known public key ciphers; it was developed by Ron Rivest, Adi Shamir, and Leonard Adleman of MIT. In the RSA cipher, Bob and Alice each generate a pair of keys; each pair has a private key and a public key. To send a secure message to Alice, Bob obtains Alice's public key and encrypts the message with it. Only Alice's private key can be used to decrypt the message. RSA is vulnerable to brute-force attacks (attempts to calculate the private key from the public key) if insufficient bits are used to calculate the keys. In practice, a minimum key length of 1024 bits ensures "unbreakability" with current and near-term computing capabilities. RSA is also vulnerable to man-in-the-middle attacks if Eve can intercept communications between Alice and Bob and make Alice and Bob believe that the substituted keys actually belong to each other. Various features of the public key infrastructure system (PKI) prevent such attacks.
Elliptic curve	Like RSA, the elliptic curve (E-C) cipher uses a pair of keys. However, a different mathematical system—this one based on the algebra of elliptic curves of large finite fields—is used to calculate the keys. To some extent, this system eliminates the type of brute-force attacks which are based on advances in factoring large numbers and to which RSA is vulnerable. Due to the increased mathematical complexity, E-C keys can be shorter than RSA keys for a given level of security. E-C is used in various products, including OpenSSL, Bouncy Castle (a set of

	programming libraries for Java and C#), and the .NET framework.
ElGamal	ElGamal is an encryption algorithm used to generate the asymmetric keys used in a public key encryption system. This algorithm was developed by Taher Elgamal in 1984. The keys are generated using the mathematical principle of the cyclic group. ElGamal is used in recent versions of PGP (Pretty Good Privacy), GNU Privacy Guard, and other systems.
DSA	The Digital Signature Algorithm is an asymmetric encryption system designed for digitally signing communications. It is not used for general-purpose encryption. It is a U.S. government standard developed in 1991 by the NIST (National Institute of Standards and Technology).