RSA Algorithm

Diffie and Hellman gave the idea of public key algorithms in 1976, but it took real shape when three MIT researchers, Rivest, Shamir, and Aldeman, came up with the RSA algorithm (named after its inventors). The algorithm was first published in 1978 and it is almost the de facto standard today.

RSA is the first and the most popular public-private key method. The algorithm is narrated below.

1. Pick up two large prime numbers, let us call them p and q (as mentioned, it has to be 1024 bits; 2048 bits is even better[32])
2. Calculate the values of $n = p \times q$ and $z = (p - 1) \times (q - 1)$
3. Find out a number d such that it is relatively prime to z. That means z should have no common factors with d except 1. This d should be less than n[33].
4. Now find out another number e such that $(e \times d - 1)$ is exactly divisible by z. It means, if we divide ed by z, the remainder will be 1. Thus e is chosen such that ed mod $z = 1$. This is sometimes represented as $ed = 1$ mod z. It is better written as $ed = 1 \pmod{z}$ indicating modulo z arithmetic. Basically it says that $ed = 1$ in modulo z arithmetic.
5. After this, we will have blocks of plaintext to send. The block size is decided such that the plaintext block P is less than n. The ciphertext is calculated as $C = P^e \pmod{n}$ and sent across to the receiver.
6. The receiver will decrypt what it receives using the formula $P = C^d \pmod{n}$.