Three-Pass Protocol:

1. In cryptography, a **three-pass protocol** for sending messages is a framework which allows one party to securely send a message to a second party without the need to exchange or distribute encryption keys.
2. Such message protocols should not be confused with various other algorithms which use 3 passes for authentication.
3. It is called a *three-pass protocol* because the sender and the receiver exchange three encrypted messages.
4. The first three-pass protocol was developed by Adi Shamir (1980).
5. The basic concept of the three-pass protocol is that each party has a private encryption key and a private decryption key. The two parties use their keys independently, first to encrypt the message, and then to decrypt the message.
6. The protocol uses an encryption function *E* and a decryption function *D*. The encryption function uses an encryption key *e* to change a plaintext message *m* into an encrypted message, or ciphertext, *E(e,m)*. Corresponding to each encryption key *e* there is a decryption key *d* which allows the message to be recovered using the decryption function, *D(d,E(e,m))=m*.
7. Sometimes the encryption function and decryption function are the same.
8. In order for the encryption function and decryption function to be suitable for the *three-pass protocol* they must have the property that for any message *m*, any encryption key *e* with corresponding decryption key *d* and any independent encryption key *k*, $D(d,E(k,E(e,m))) = E(k,m)$.
9. In other words, it must be possible to remove the first encryption with the key *e* even though a second encryption with the key *k* has been performed. This will always be possible with a commutative encryption.
10. A commutative encryption is an encryption that is order-independent,
    i.e. it satisfies $E(a,E(b,m))=E(b,E(a,m))$
    for all encryption keys *a* and *b* and all messages *m*. Commutative encryptions satisfy
    $D(d,E(k,E(e,m))) = D(d,E(e,E(k,m))) = E(k,m)$.

The three-pass protocol works as follows:

1. The sender chooses a private encryption key s and a corresponding decryption key t. The sender encrypts the message m with the key s and sends the encrypted message E(s,m) to the receiver.
2. The receiver chooses a private encryption key r and a corresponding decryption key q and super-encrypts the first message E(s,m) with the key r and sends the doubly encrypted message E(r,E(s,m)) back to the sender.
3. The sender decrypts the second message with the key t. Because of the commutatively property described above D(t,E(r,E(s,m)))=E(r,m) which is the message encrypted with only the receiver's private key. The sender sends this to the receiver.

The receiver can now decrypt the message using the key q, namely D(q,E(r,m))=m the original message.
Notice that all of the operations involving the sender's private keys s and t are performed by the sender, and all of the operations involving the receiver's private keys r and q are performed by the receiver, so that neither party needs to know the other party's keys.

Shamir three-pass protocol

The first three-pass protocol was the Shamir three-pass protocol developed in 1980. It is also called the *Shamir No-Key Protocol* because the sender and the receiver do not exchange any keys, however the protocol requires the sender and receiver to have two private keys for encrypting and decrypting messages. The Shamir algorithm uses exponentiation modulo a large prime as both the encryption and decryption functions. That is $E(e,m) = m^e \bmod p$ and $D(d,m) = m^d \bmod p$ where *p* is a large prime.

For any encryption exponent *e* in the range 1..*p*-1 with gcd(*e*,*p*-1) = 1.
The corresponding decryption exponent *d* is chosen such that $de \equiv 1 \pmod{p-1}$. It follows from Fermat's Little Theorem that $D(d,E(e,m)) = m^{de} \bmod p = m$.

The Shamir protocol has the desired commutatively property since
$E(a,E(b,m)) = m^{ab} \bmod p = m^{ba} \bmod p = E(b,E(a,m))$.

Fermat's little theorem states that if p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p. In the notation of modular arithmetic, this is expressed as

$$a^p \equiv a \pmod{p}.$$

For example, if $a = 2$ and $p = 7$, then $2^7 = 128$, and $128 - 2 = 126 = 7 \times 18$ is an integer multiple of 7.

If a is not divisible by p, Fermat's little theorem is equivalent to the statement that $a^{p-1} - 1$ is an integer multiple of p, or in symbols:[1][2]

$$a^{p-1} \equiv 1 \pmod{p}.$$

For example, if $a = 2$ and $p = 7$, then $2^6 = 64$, and $64 - 1 = 63 = 7 \times 9$ is thus a multiple of 7.