Your outlined workflow for online payment is a good starting point and covers the basic steps involved in the process. Encryption plays a vital role in ensuring the security and confidentiality of data throughout this flow. Here’s an adjusted version of your workflow with emphasis on encryption and some additional security measures:

1. \*\*Selection of Goods:\*\*

- The user browses and selects the items they wish to purchase.

2. \*\*Checkout and Payment Page:\*\*

- Upon proceeding to checkout, the connection transitions to a secure HTTPS (TLS/SSL) connection if it hasn't already.

- The TLS/SSL protocols encrypt the data transmitted between the user’s browser and the merchant’s server, ensuring that sensitive information remains confidential.

3. \*\*Entry of Card Information:\*\*

- The user enters their card information.

- Tokenization is employed to replace sensitive card data with a unique identifier (token), reducing the risk associated with handling and storing sensitive information on the merchant’s system.

4. \*\*User Authentication:\*\*

- Multi-factor authentication (MFA) is initiated to verify the user’s identity. This could be an OTP sent via SMS, as you mentioned, or other methods like biometric verification or a mobile app prompt.

5. \*\*Payment Authorization:\*\*

- The payment gateway contacts the card issuer (e.g., bank) to authorize the payment.

- Encryption is again crucial here as it ensures that the communication between the payment gateway, the merchant, and the card issuer remains secure.

6. \*\*Payment Processing:\*\*

- Once authorized, the payment is processed, and the funds are transferred from the user’s account to the merchant’s account.

7. \*\*Confirmation:\*\*

- The merchant sends a confirmation receipt to the user, and the user is notified that the transaction has been completed successfully.

In this revised workflow, encryption is employed in several steps to ensure the confidentiality and integrity of data. It's used in the TLS/SSL connection to secure data transmission between the user and the merchant, in tokenization to secure card information, and in the communication between the payment gateway, the merchant, and the card issuer during payment authorization and processing.

Incorporating these encryption technologies and security measures can significantly enhance the security posture of the online payment process.