**Write a brief explanation (200 words) on how HTTPS improves security over HTTP.**

HTTPS enhances security compared to HTTP by using encryption and authentication to protect data between users and servers. The key difference is that HTTPS employs Transport Layer Security (TLS) to encrypt the information being sent, making sensitive data – like passwords and credit card numbers—unreadable. This encryption prevents malicious actors from easily intercepting and understanding the data during transmission.

In addition to encryption, HTTPS verifies the identity of the web server through SSL certificates. These certificates confirm that the server a user connects to is genuine, helping to stop attacks such as phishing, man-in-the-middle (MitM) attacks, and domain spoofing. When users visit a website with HTTPS, their browser checks the SSL certificate to ensure the server is legitimate, which builds trust.

By protecting data through encryption and confirming the server's identity, HTTPS increases user confidence and promotes safer online experiences. This is especially important in today’s digital world, where cyber threats are common. Overall, using HTTPS is essential for any website that handles sensitive information, ensuring that data remains secure and maintaining user trust.