SSL

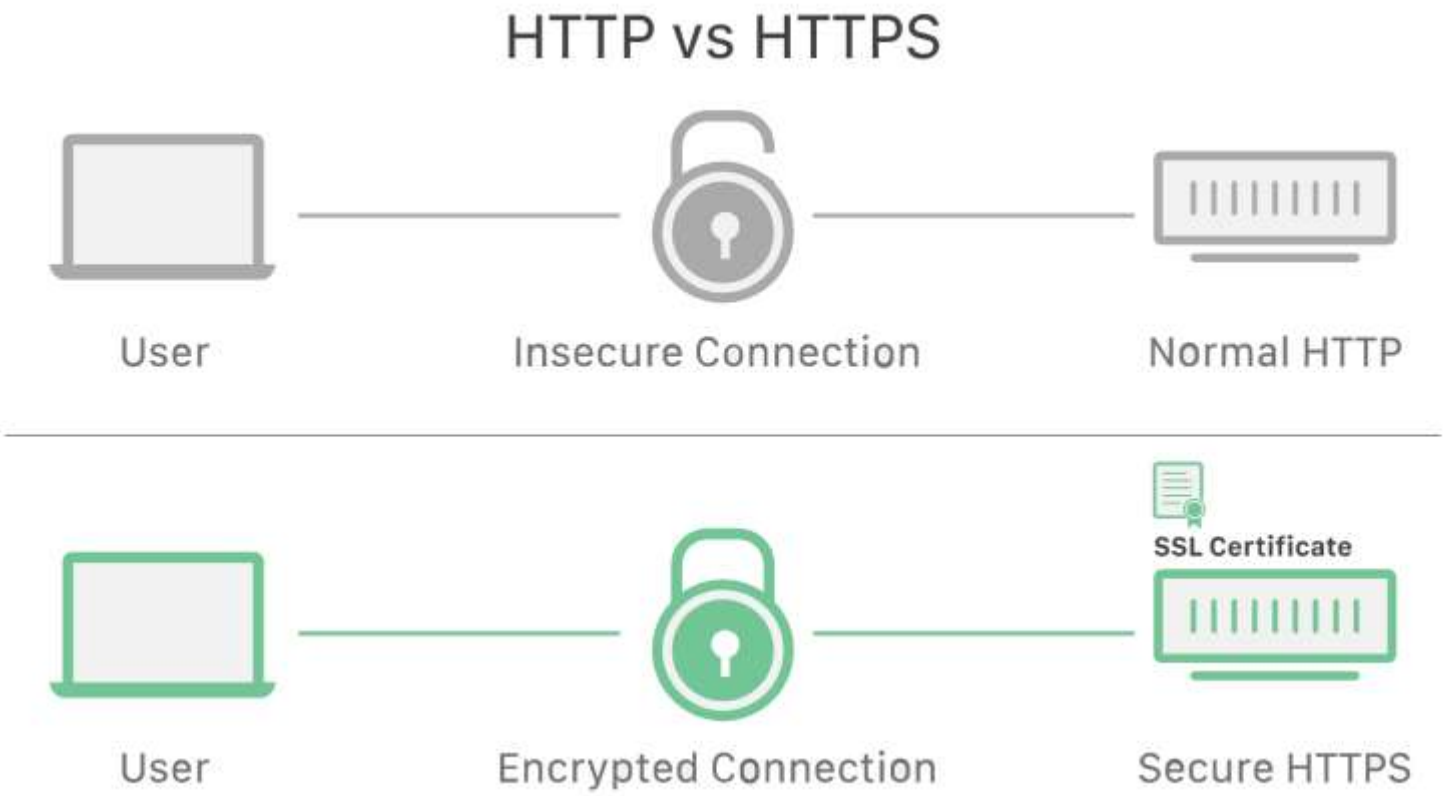
IESED
Co-funded by the Erasmus+ Programme of the European Union

SCHOOL OF BUSINESS OF BSU

+ HTTPS => + Google Rating (с 01.10.2019)

SSL (Secure Sockets Layer)

It is a standard security technology for establishing encrypted communication between a web server and a browser [https://www.cloudflare.com/learning/ssl/what-is-ssl/].



This link ensures that all data passed between the web server and browsers remain private and integral.

Eg. (https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/), suppose we take a text message «Hello» and encrypt it with a key *;

For example "2jd8932kd8". Encrypted with this key, our simple «hello» now is «X5xJCSycg14 =», what looks like random garbage data.

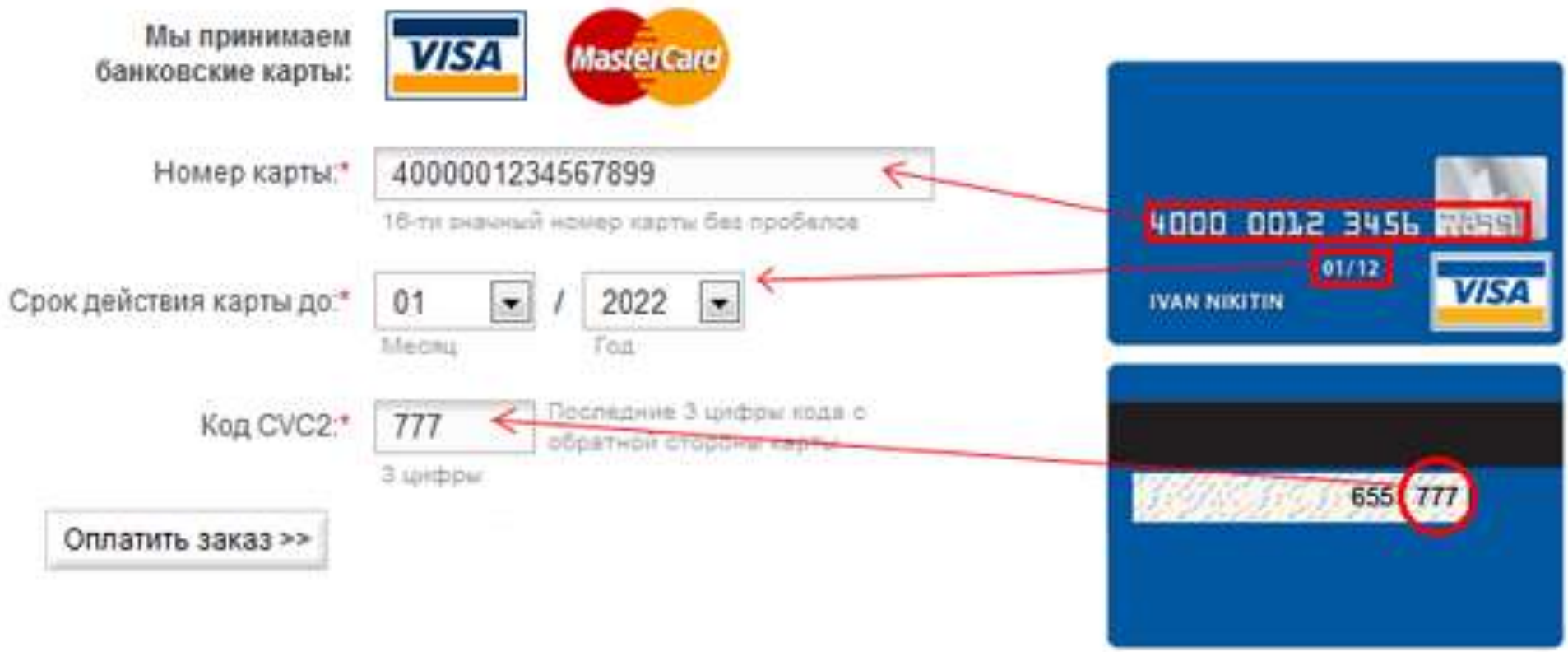
However, having decrypted it with the same key, we get the word “hello” back.

Clear text + key = Encrypted_text

hello + 2jd8932kd8 = X5xJCSycg14 =

Encrypted_text - key = plaintext

X5xJCSycg14 - 2jd8932kd8 = hello



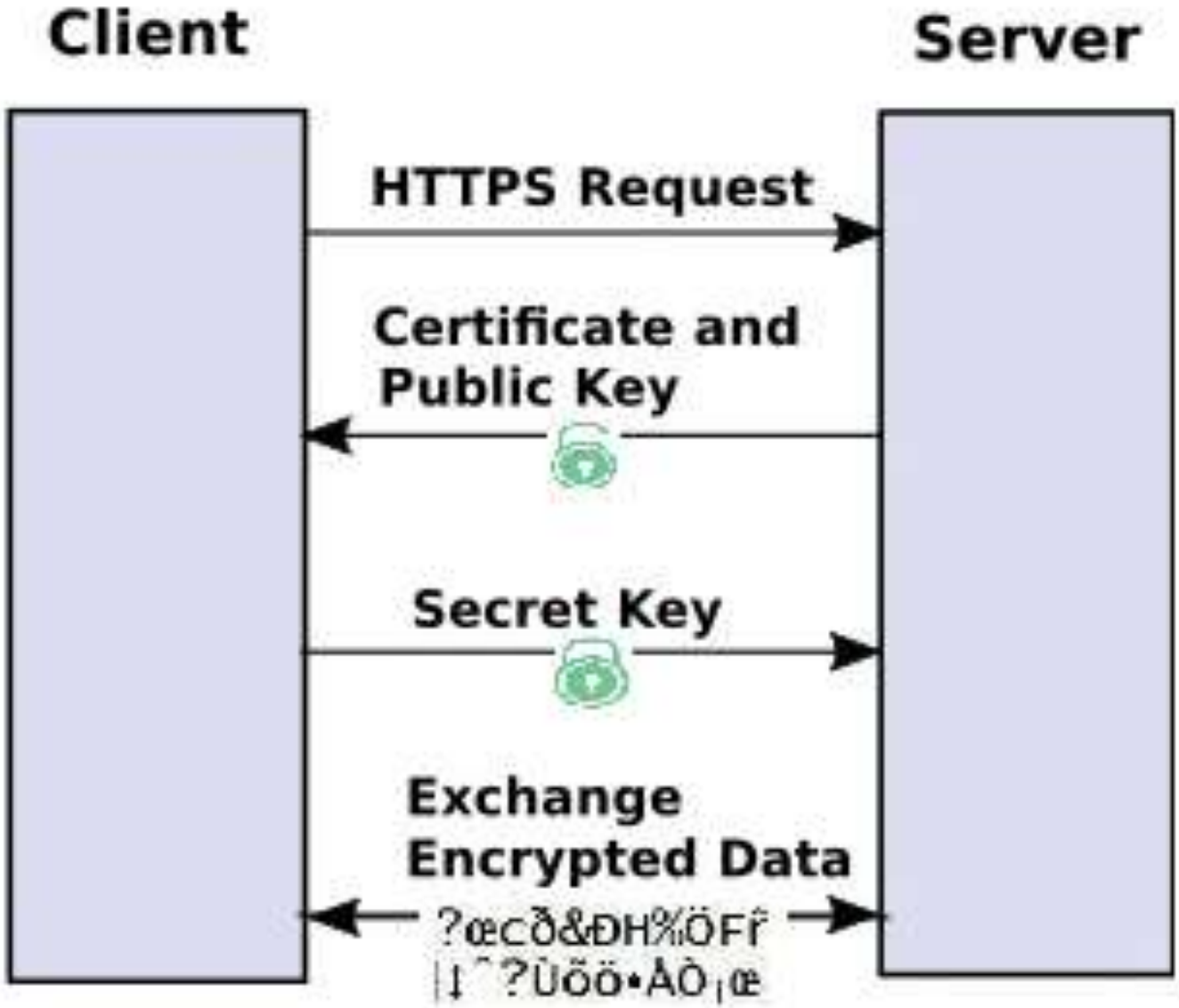
http://sberbank.com? Number=**4000001234567899**& Date=**01/2022**& CVC2=**777**

https://sberbank.com?

Number=
4000001234567899
&
Date=**01/2022**
&
CVC2=**777**

looks like random garbage data.

\+ **authenticity** in each transaction


Client
Server
HTTPS Request
Certificate and
Public Key
Secret Key
Exchange
Encrypted Data
?œCð&ÐH%ÖFî
|↓ ˆ?Ùõö•ÅÒ¡œ

The browser connects to a web server (website), that is secured with SSL (https).

The browser requests that the server identify itself.

Server sends a copy of its SSL certificate, including the server’s public
key.

The browser checks the root directory of the certificate in accordance with the list of trusted certificate authorities, and also that the certificate has not expired, it has not been revoked and its common name is valid for the website to which it connects. If the browser trusts the certificate, it creates, encrypts, and sends back the symmetric session key using the server's public key.

The server decrypts the symmetric session key using its private key, and sends back the confirmation, encrypted using the session key, to start the encrypted session.

The server and browser now encrypt all transmitted data using the session key.

https://sberbank.com?
Number=
4000001234567899 <==>
&
Date=**01/2022**
&
CVC2=**777**

p»┤X!æ⊢›½─ί┬‰|ΕŁε
B¡k†,?œcð&ÐH%ÖFf
œœ?9+↕^?Ùõö•ÅÒ┐œ
ã&ã┬@JÂ¼–*↑>–└|‼k
õ¦e¾©´┘þ•ëÞ«‰E´_
ïr÷d~»±“üÙ™8´└Rá
*ötUÅïMÑz ├H:%Sž
┬n;§”_/Å`÷Ï84Ò¬
y*³àdðìš~|~↕ªžkl
e¯ôsÉëh$ ¼:4pu~l