Page 133-134

2. b
4. c
6. b
8. b
10. a
12. a
14. c
16. c
18. c
20. b

Page 181-183

1. d
3. d
5. a
7. b
9. c
11. c
13. b
15. a
17. d
19. b

Case Project 3-2

The 3 cipher tools are as follows:

Caesarian shift:

This is an easy shift cipher that is simple to crack. It takes the place of a letter by shifting the alphabet backwards, to the first letter of the alphabet. Decrypt GFRGHA with a 3 shift, for instance. Look three letters ahead of G to decipher it: D. As a result, G may be decoded using D.

ROT13 :

This aids in redistributing the 13 forwarded letters evenly throughout the group. ROT13 is a simple cipher, yet it outperforms the other three in terms of security.

Cryptogram solver :

It's an encryption based on letter substitutions.

For example, the cipher: hello how are you, Has the following solution:

AFOOT ATS ELF BTU
AFOOT ATS REF BTU
AFOOT ATS REF LTD
AFOOT ATS ELF NTH
AFOOT ATS REF NTH
ALOOF AFT DEL IFS

So, the cryptogram solver is difficult to be used.

Case Project 4-4

HTTPS (HyperText Transfer Protocol Secure) is an extension of HTTP that enhances network security by encrypting data in transit, in detail, adding TLS/ SSL encryption to encrypt HTTP request and response. As a result, HTTPS is used to protect client and server data from tampering and assure the integrity, security, and privacy of that data in transit. HTTPS offers three layer levels of security over HTTP, making it more secure:

- Encryption: It protects the data being sent from unauthorized access by preventing a third party from reading it.
- Ensures that data is not altered during transmission between client and server.
- Authentication : This guarantees that only authorized users can retrieve data.

HTTPS has the following advantages:

- HTTPS encrypts all transmitted data so it protects the data.
- HTTPS can protects the connections against phishing and other frequent data breaches.
- HTTPS secures the connection by encrypting it and utilizing server authentication.

HTTPS has the following disadvantages:

- Because of the more complex SSL encryption and decryption processes utilized, HTTPS-enabled websites load slower.
- HTTPS will result in an increase in processing resources costs.

Following is an explanation of HTTP vs HTTPS ：

HTTP	HTTPS
To provide transportation of information over a network.	An extension of HTTP for securer network communication.
Port 80	Port 443
Operates on the application layer.	Operates on the transport layer.
Not required	HTTPS requires the SSL/TLS encryption.
Faster	Slower
Not required	Domain validation

To enable https, perform the following steps on the server:

- A dedicated server with a dedicated IP address is required to increase security and set up SSL certification.
- The certificate proves the legitimate owner of the domain.
- The web host will activate the certificate.
- The certificate should be installed.
- Update the site over to HTTPS.

If people are on a public wi-fi network and accessing an insecure website, their data is at risk of being stolen and misused. The fact that HTTPS is secure means that data is better protected because the integrity and confidentiality of data are preserved. As with DNS queries, HTTPS ensures that the connection is encrypted but does not encrypt all the data. As a result, when using public wi-fi, it's best to utilize a VPN to protect your online activities. HTTPS does not have to be used to secure all web traffic. It is determined by the website's content. On the other hand, it should be utilized if one want to keep their data private and secure.