Wireshark – captures every computer domain transaction.

Kerberos –

KCD – Key distribution centre – checks passwords

1. Request Authentication
2. Receive authentication
3. request ticket
4. receive ticket
5. Use ticket for service
6. repeat ticket request if necessary

Active Directory – user information for server

2 step – second step once you’re connected

multi factor – both steps before connection

Full Disk Encryption – password for disk and similar objects

client – PC

Terminal Server – for multiple users

Hash – irreversible encryption 128 bits long depending on

OSI – Physical – Data Link – Network – Transport – Session – Presentation – Application

TLS – level 5

SSL – remind teacher

Telnet

HTTPS

ciphertext – encrypted

algorithm – how the encryption and decryption work, the mathematic function that creates the cipher

key space – all possible keys

key – parameter in the algorithm, the secret to decrypting the cipher.

algorithm needs content and key to work

algorithm is known, key is a secret

Transposition – change letter placement

rail fence – make a grid with the message and encrypt it with the order the letters appear in a straight line after writing the plain text in a certain pattern.

columnar – make a grid and the cipher is made of columns ordered by the chosen key column position.

Substitution – change letters with others

Caesar – substitute letters randomly

Rot13 – rotate the alphabet 13 times and use those substitutes

ATBASH

Chaotic substitution – create your own alphabet by putting a keyword with unique letters and the beginning and write the rest of the alphabet without those letters.

Brute force – submit many phrases until successful

Polyalphabetic – use multiple alternative alphabets in order to encrypt a message.

Vigenere Cipher -