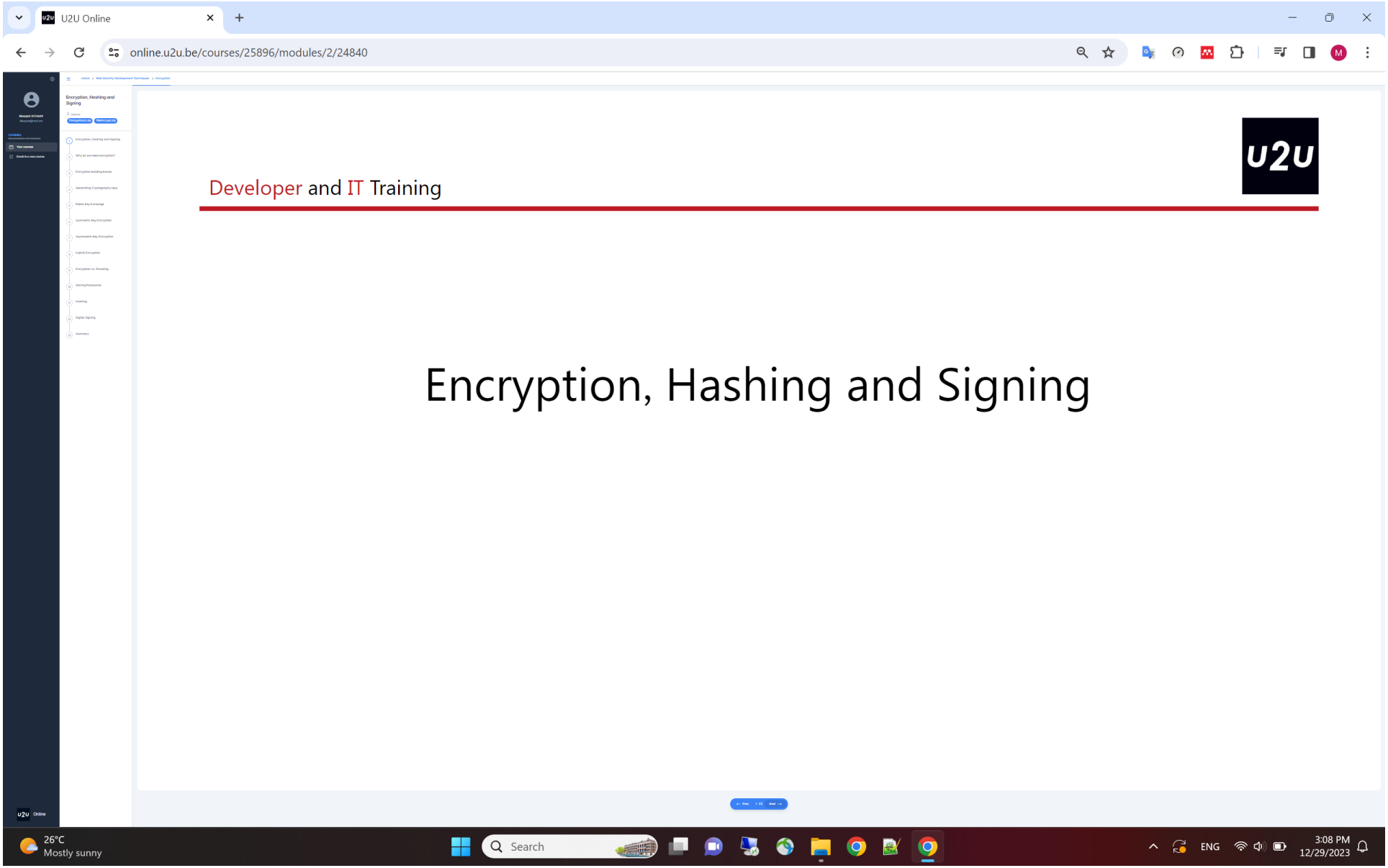

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Developer and IT Training
U2U
Encryption, Hashing and Signing
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/2/24840

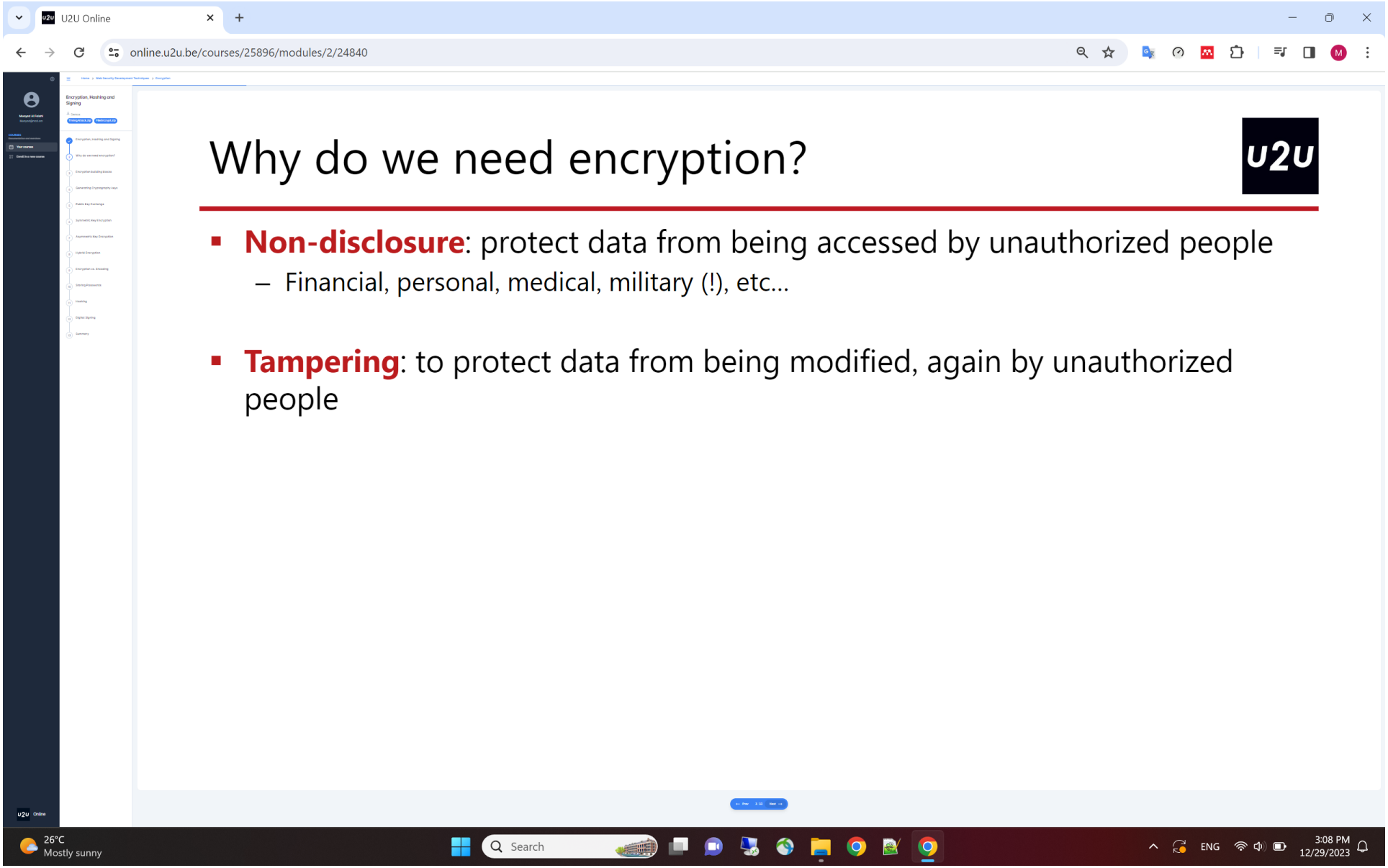
Agenda

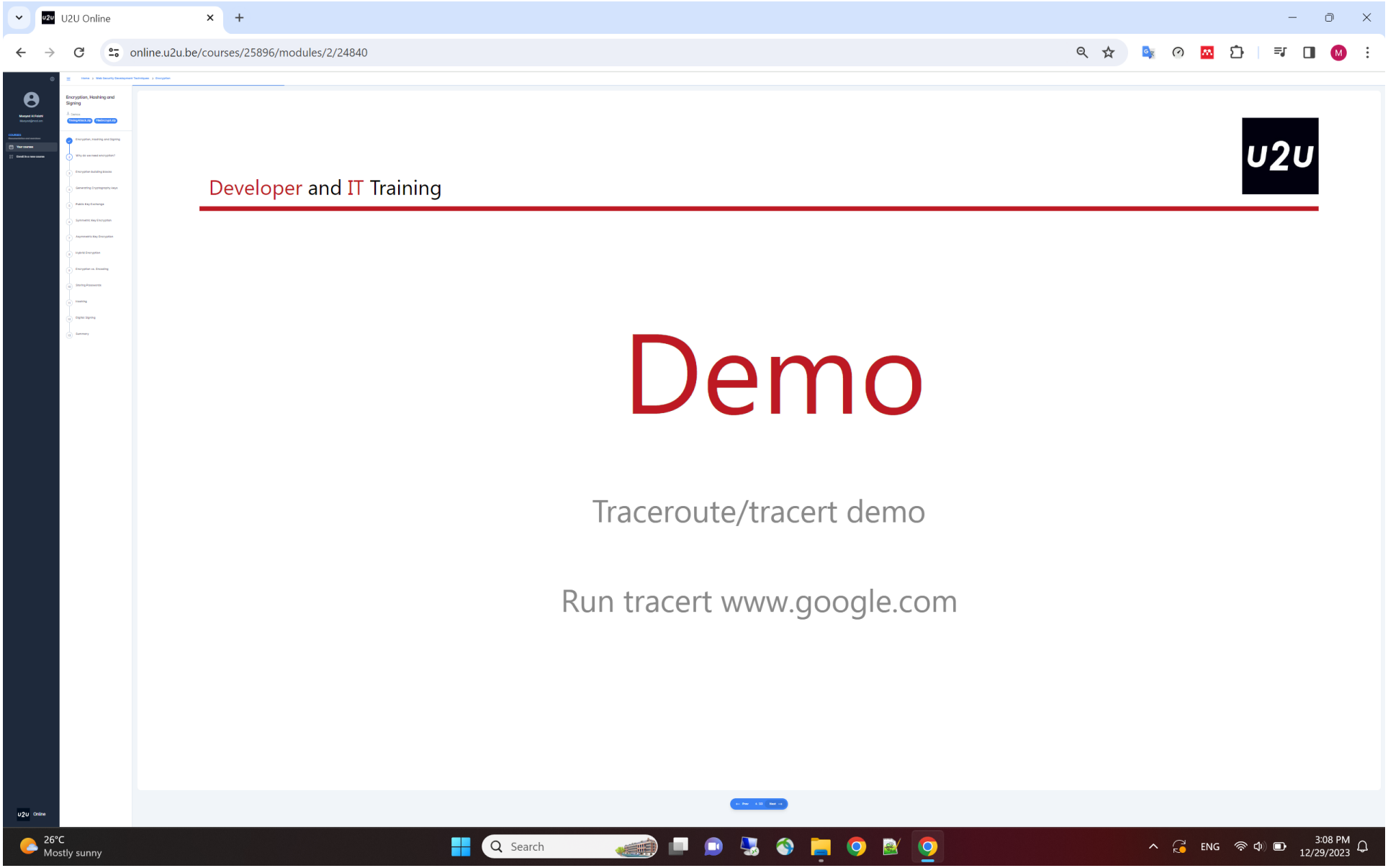
- Why do we need encryption, and what does it mean?
- Encryption building blocks
- Generating Cryptography keys
- Public Key Exchange
- Symmetric Key Algorithms
- Asymmetric Key Algorithms
- Hybrid Encryption
- Storing Passwords safely
- Hashing
- Digital Signing

26°C Mostly sunny

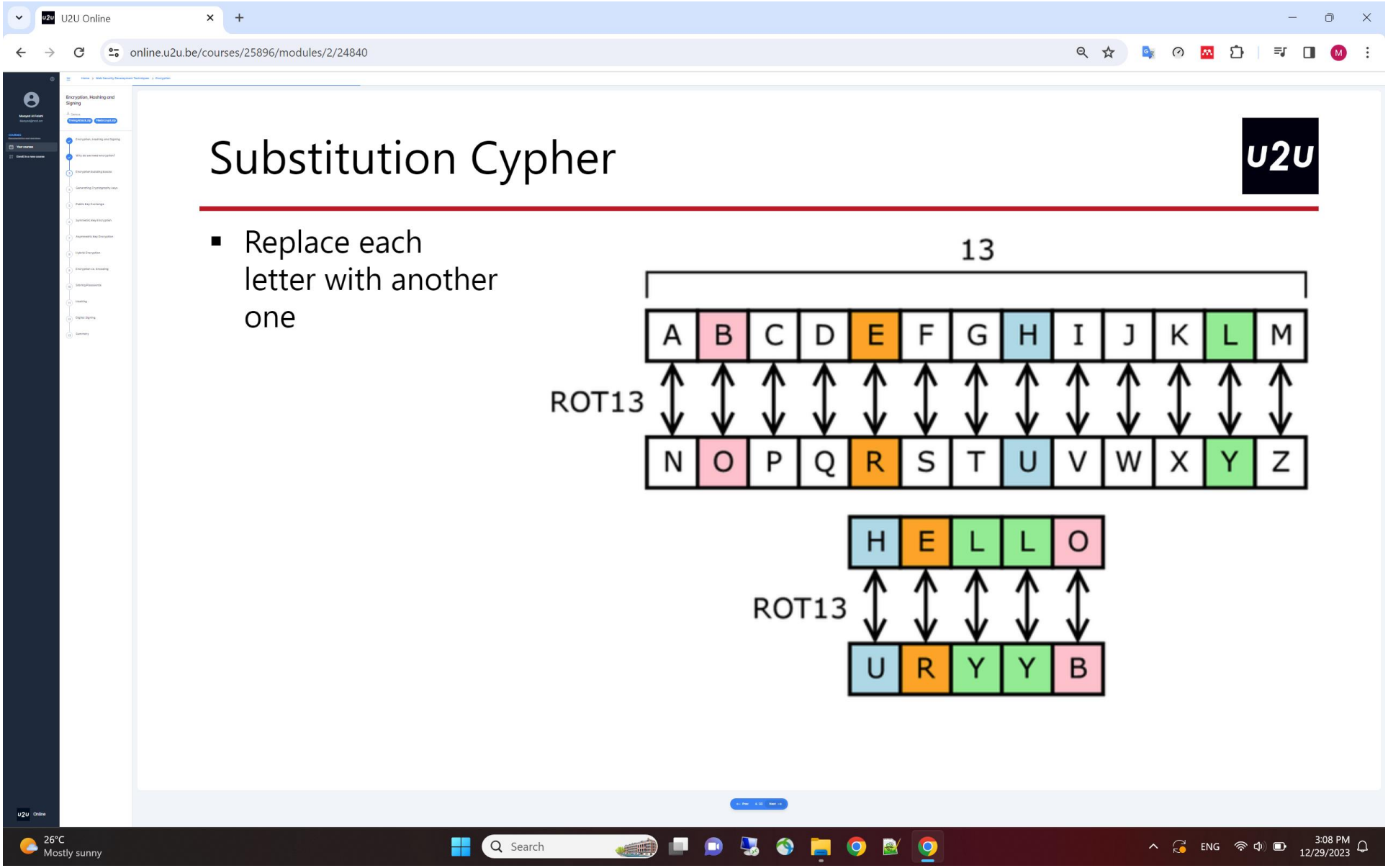
Search

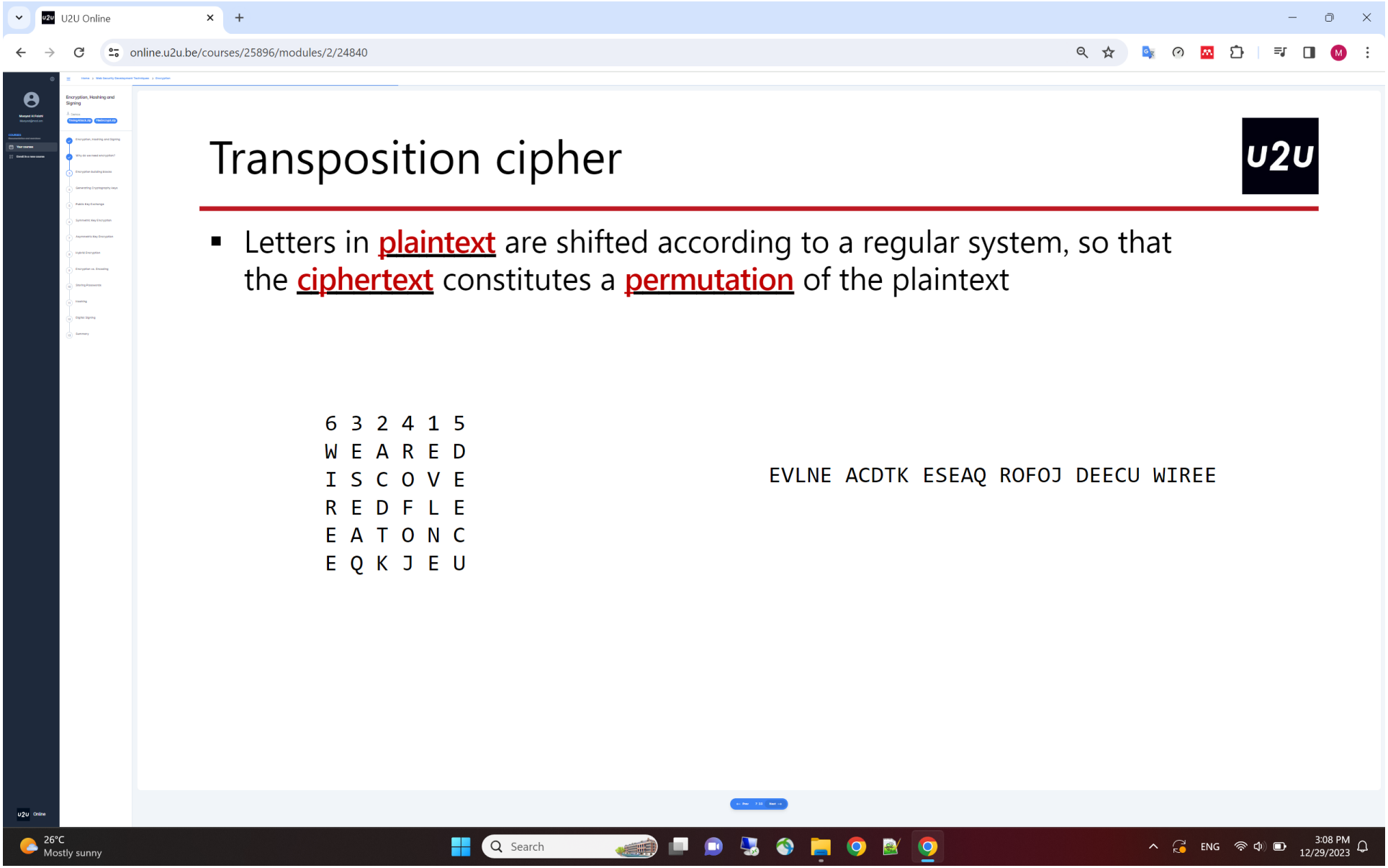
ENG 3:08 PM 12/29/2023

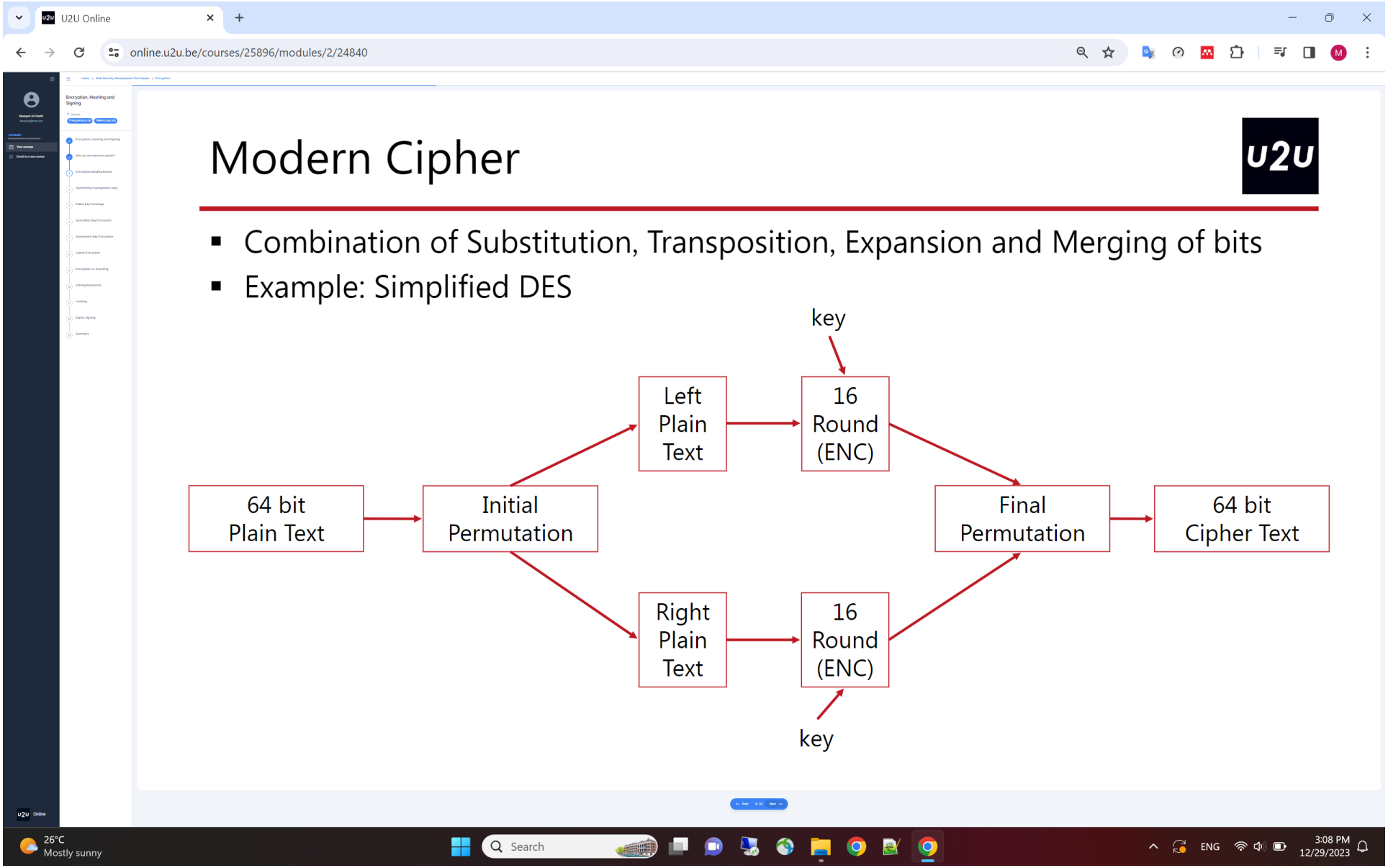

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Why do we need encryption?
U2U
Non-disclosure: protect data from being accessed by unauthorized people
Financial, personal, medical, military (!), etc...
Tampering: to protect data from being modified, again by unauthorized people
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

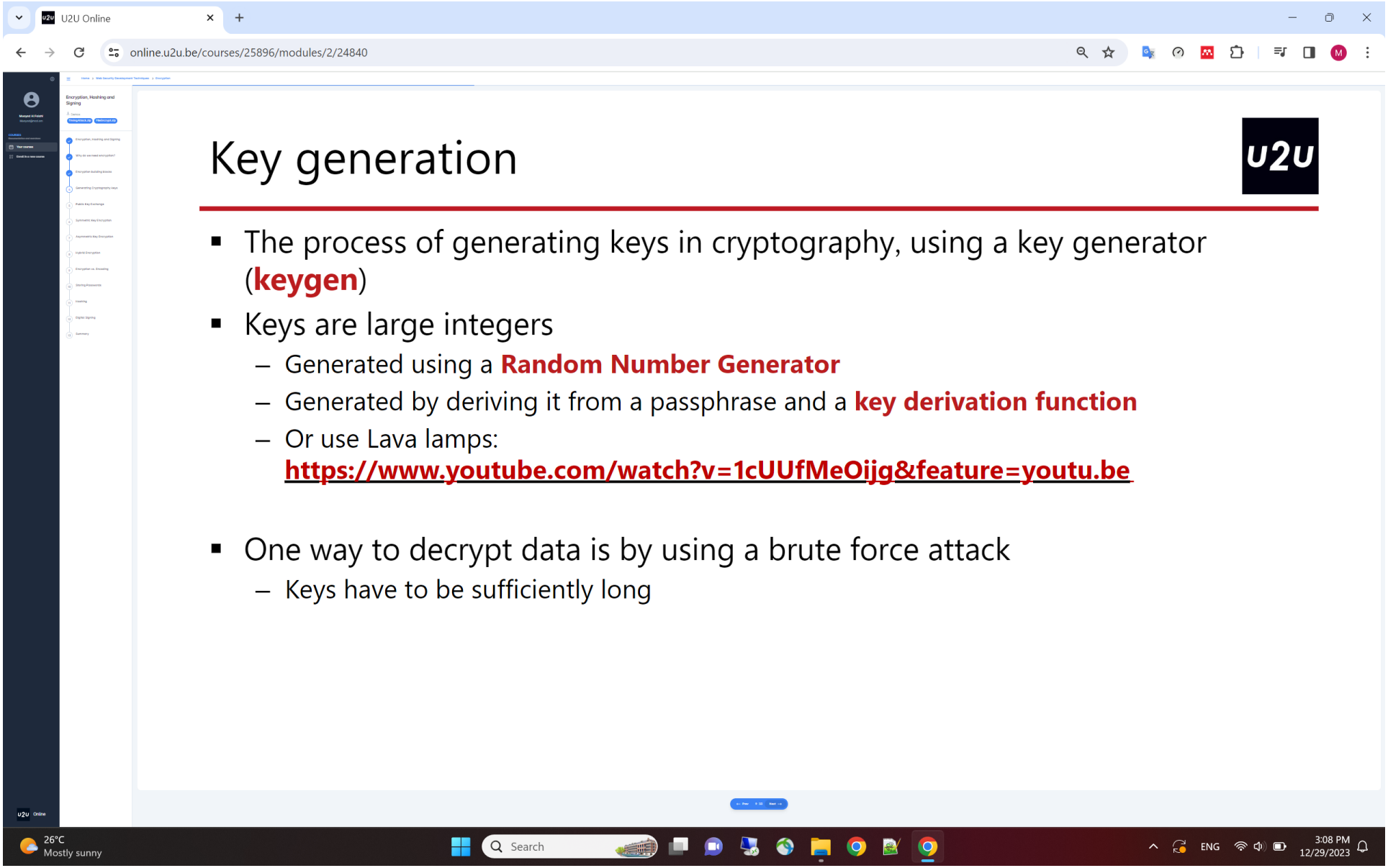

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Developer and IT Training
U2U
Demo
Traceroute/tracert demo
Run tracert www.google.com
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

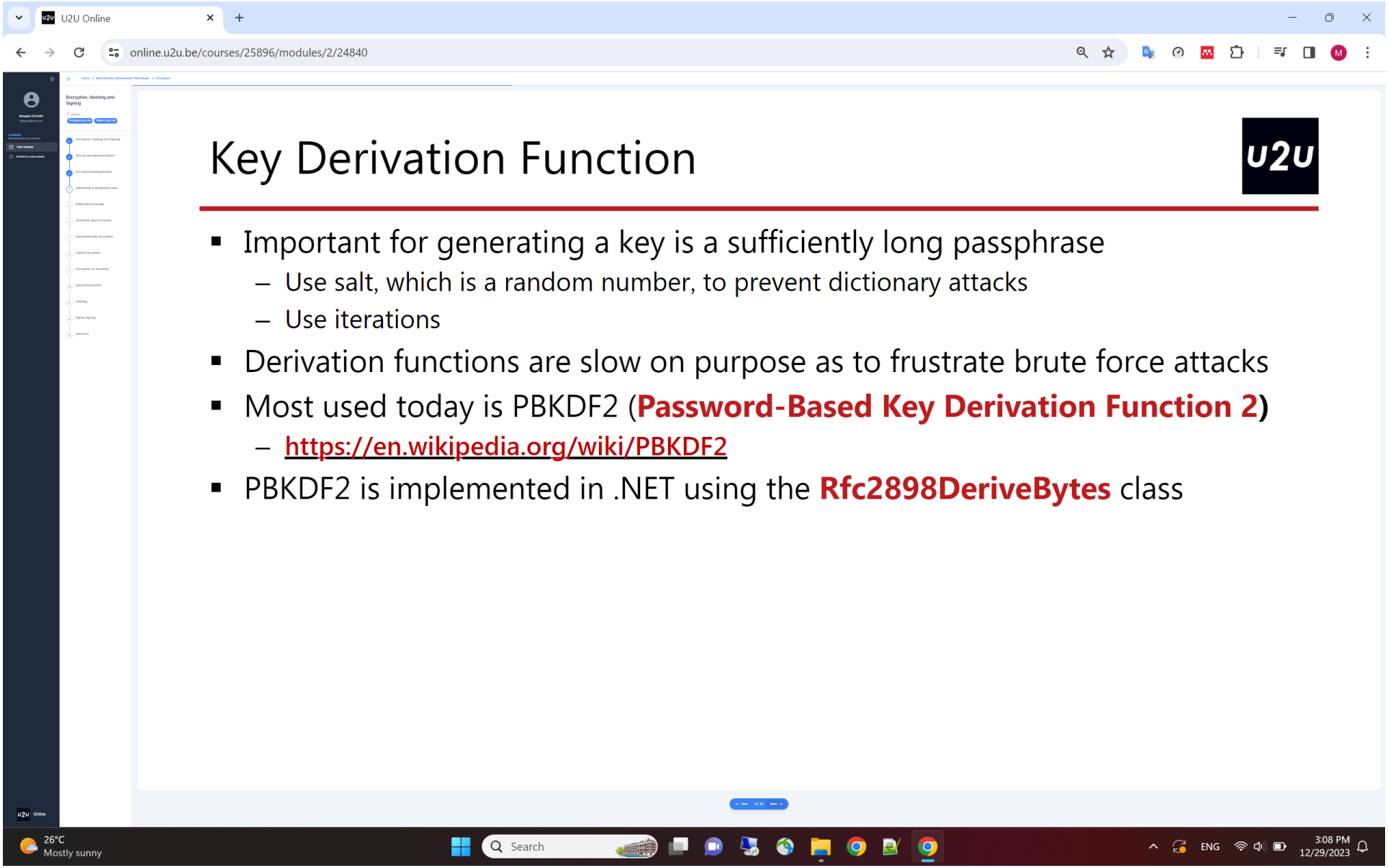

U2U Online
online.u2u.be/courses/25896/modules/2/24840
What does encryption mean?
U2U
Encryption: “Make data unreadable for third parties”
Decryption: “Make readable again”
Technically: plaintext becomes (seemingly) pure random data (cyphertext) which can become readable again using the correct cryptographic key
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

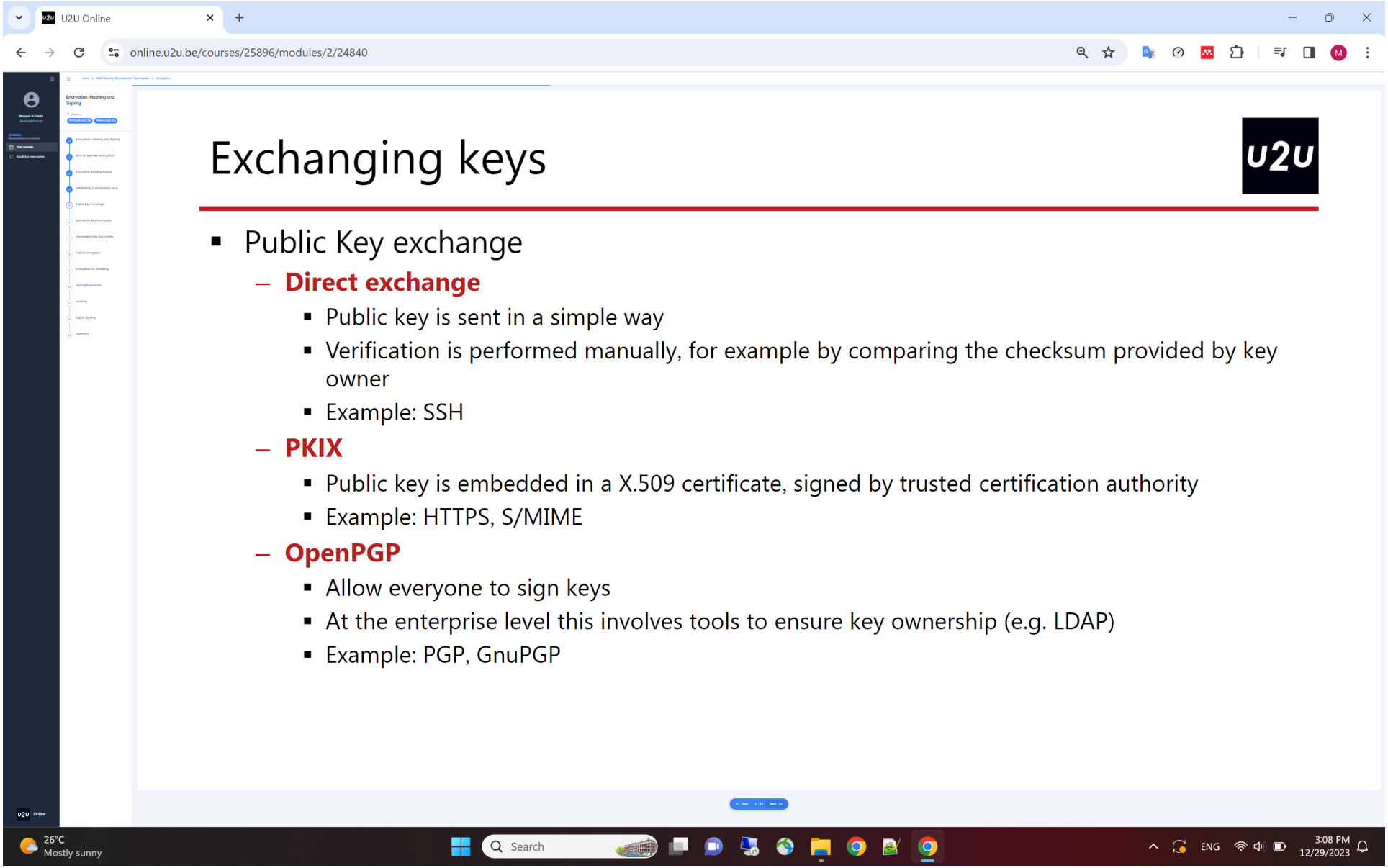

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Substitution Cypher
U2U
Replace each letter with another one
13
A B C D E F G H I J K L M
ROT13
N O P Q R S T U V W X Y Z
H E L L O
ROT13
U R Y Y B
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

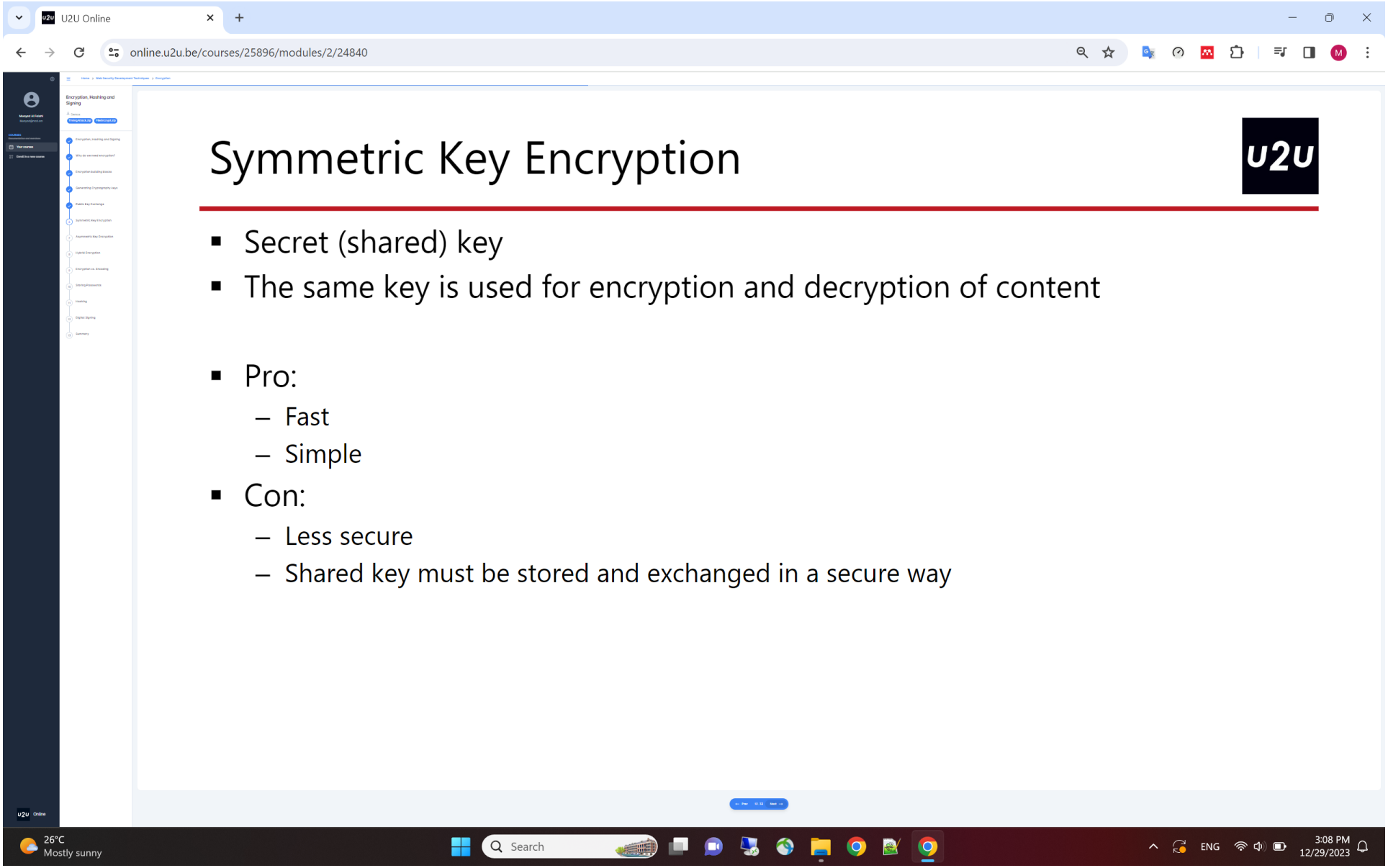

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Transposition cipher
U2U
Letters in plaintext are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U
EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

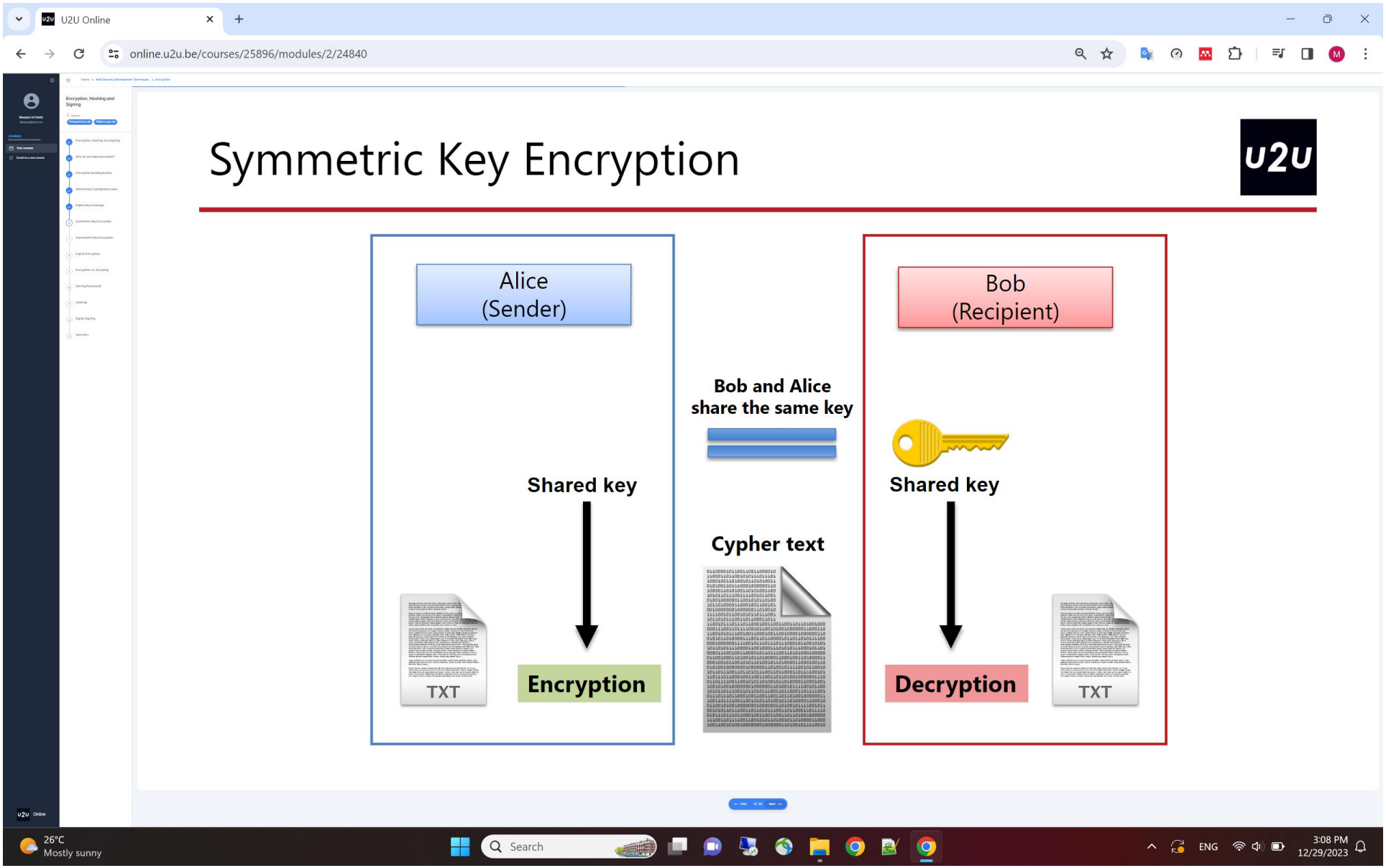

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Modern Cipher
u2u
Combination of Substitution, Transposition, Expansion and Merging of bits
Example: Simplified DES
key
Left Plain Text
16 Round (ENC)
64 bit Plain Text
Initial Permutation
Final Permutation
64 bit Cipher Text
Right Plain Text
16 Round (ENC)
key
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

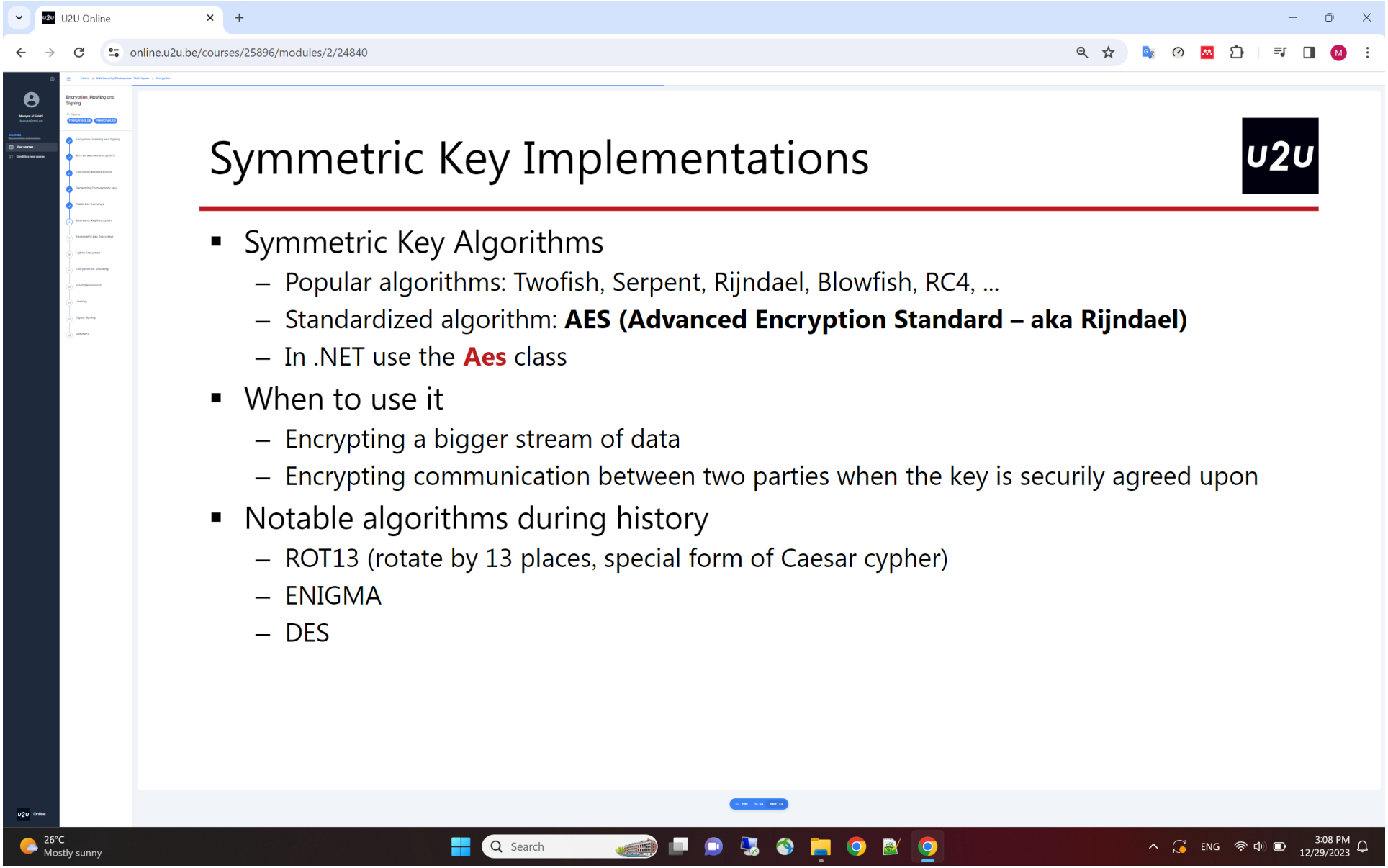

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Key generation
U2U
The process of generating keys in cryptography, using a key generator (keygen)
Keys are large integers
Generated using a Random Number Generator
Generated by deriving it from a passphrase and a key derivation function
Or use Lava lamps: https://www.youtube.com/watch?v=1cUUfMeOijg&feature=youtu.be
One way to decrypt data is by using a brute force attack
Keys have to be sufficiently long
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

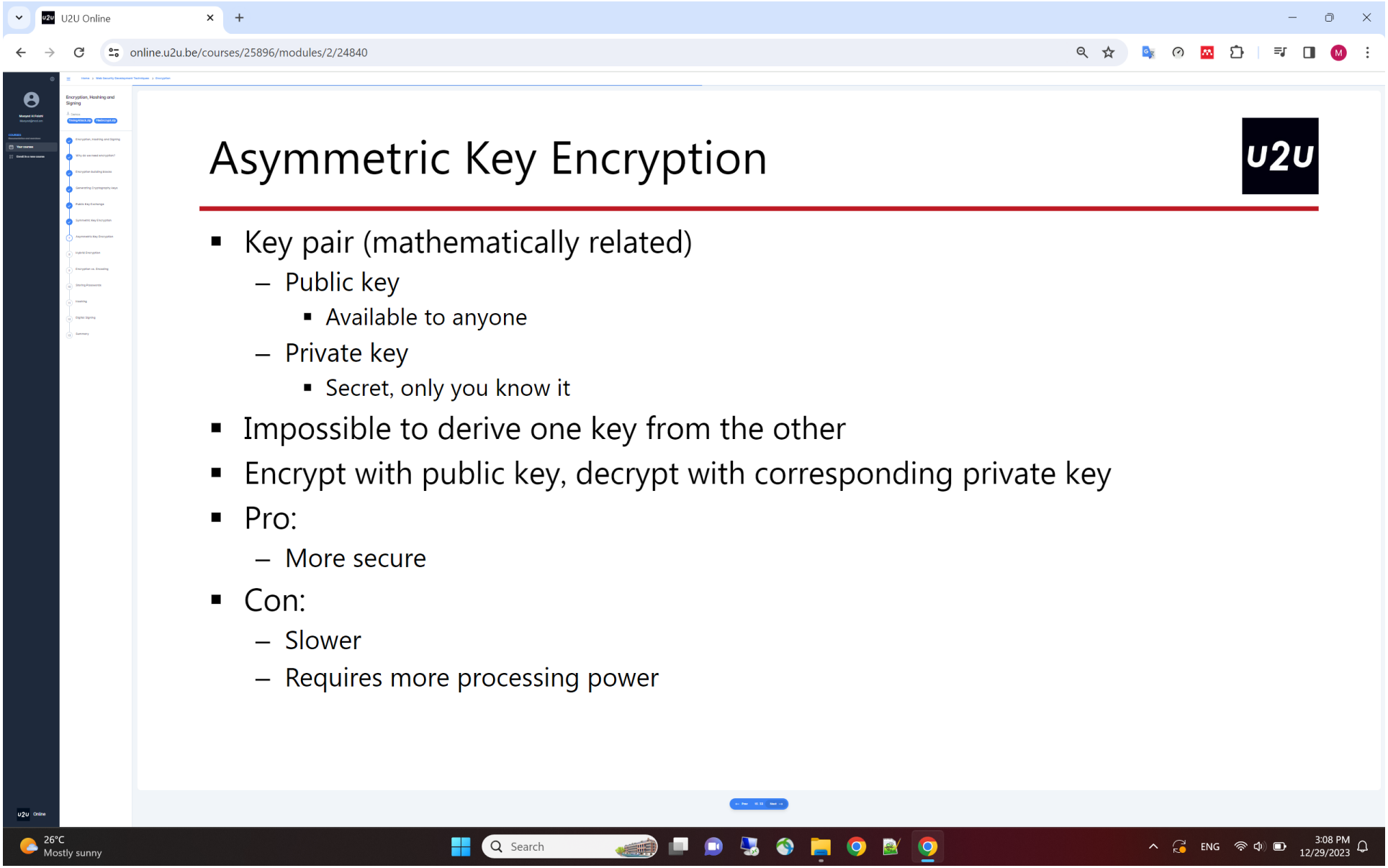

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Key Derivation Function
U2U
Important for generating a key is a sufficiently long passphrase
Use salt, which is a random number, to prevent dictionary attacks
Use iterations
Derivation functions are slow on purpose as to frustrate brute force attacks
Most used today is PBKDF2 (Password-Based Key Derivation Function 2)
https://en.wikipedia.org/wiki/PBKDF2
PBKDF2 is implemented in .NET using the Rfc2898DeriveBytes class
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

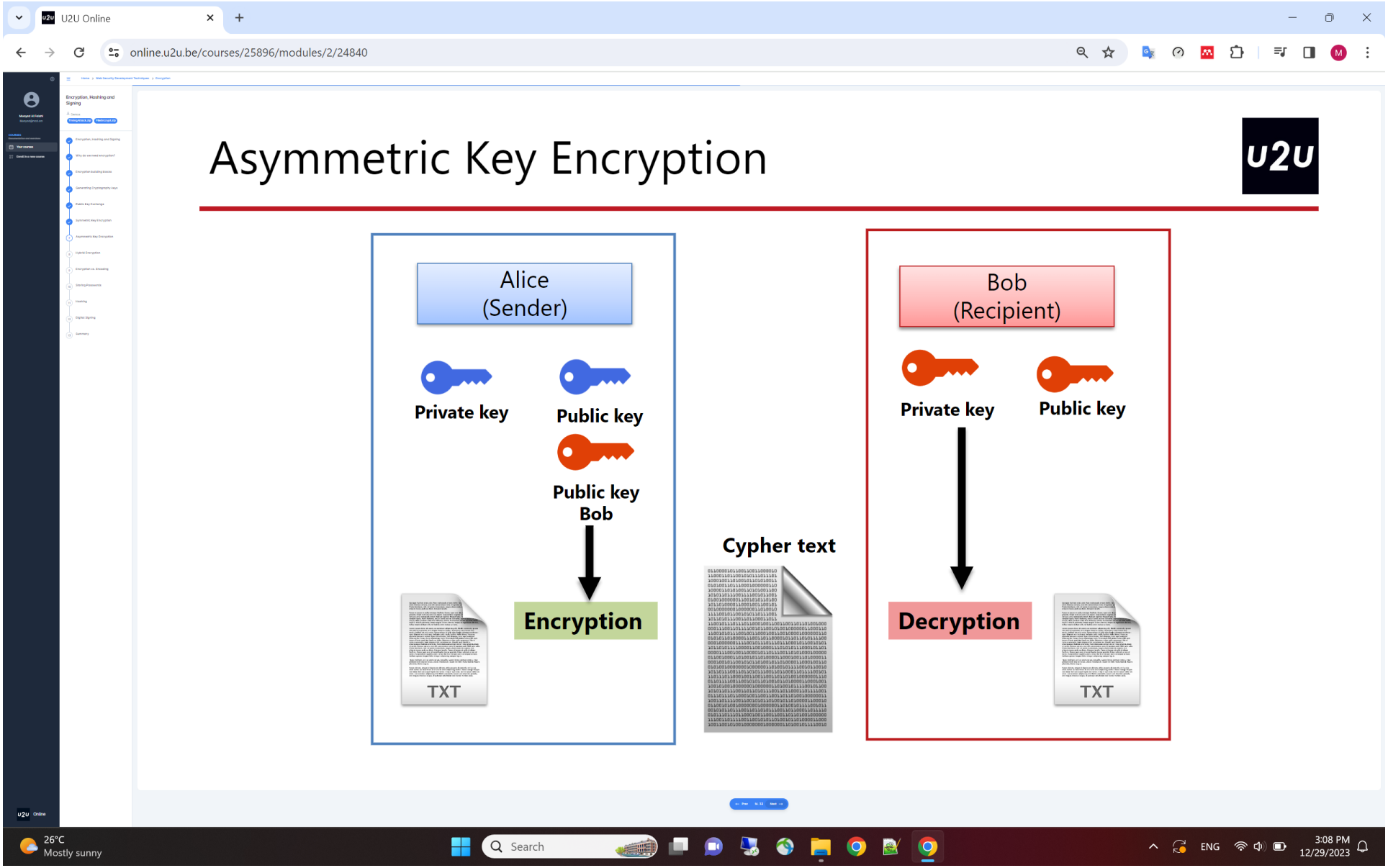

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Exchanging keys
u2u
Public Key exchange
Direct exchange
Public key is sent in a simple way
Verification is performed manually, for example by comparing the checksum provided by key owner
Example: SSH
PKIX
Public key is embedded in a X.509 certificate, signed by trusted certification authority
Example: HTTPS, S/MIME
OpenPGP
Allow everyone to sign keys
At the enterprise level this involves tools to ensure key ownership (e.g. LDAP)
Example: PGP, GnuPGP
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

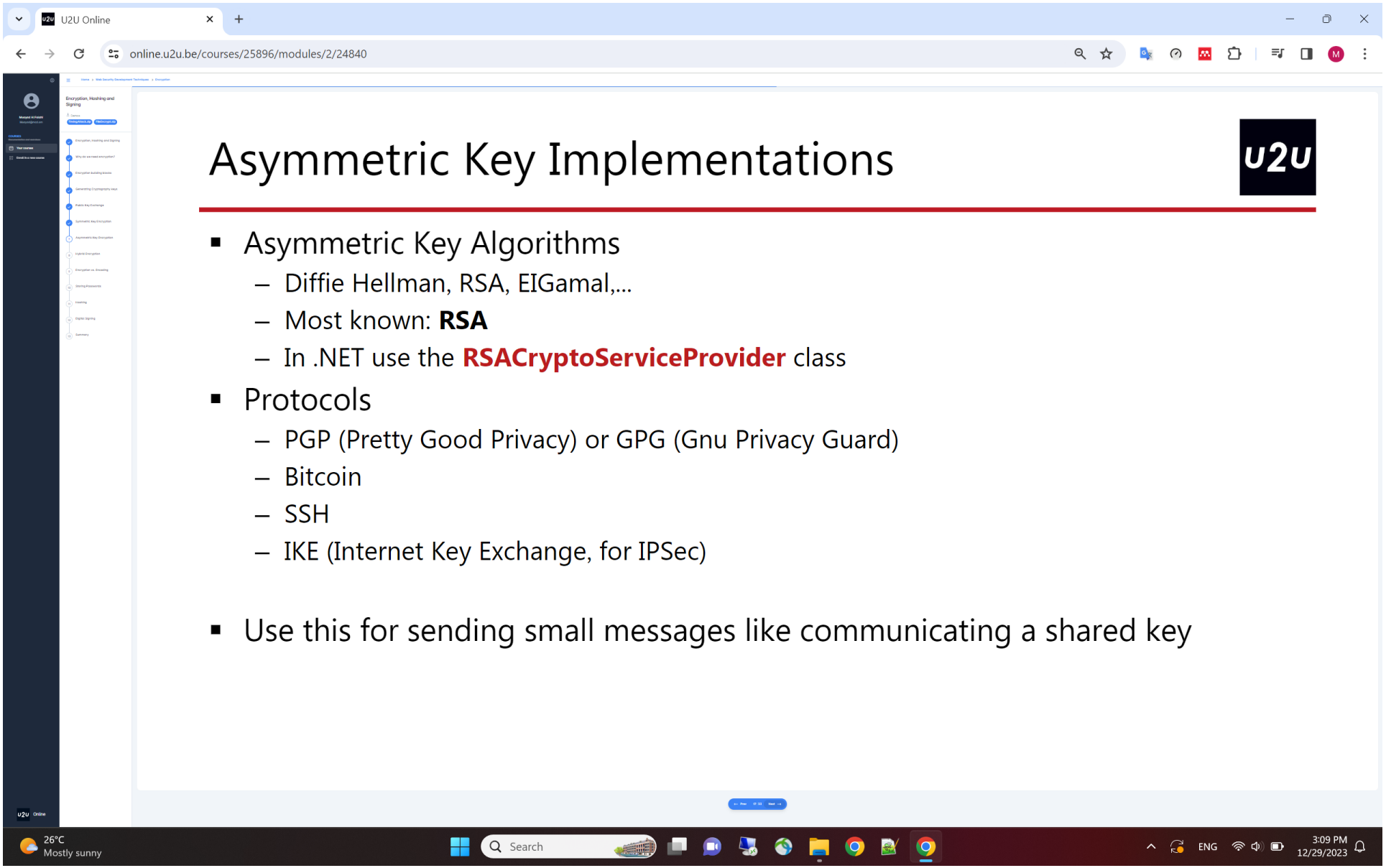

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Symmetric Key Encryption
u2u
Secret (shared) key
The same key is used for encryption and decryption of content
Pro:
Fast
Simple
Con:
Less secure
Shared key must be stored and exchanged in a secure way
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

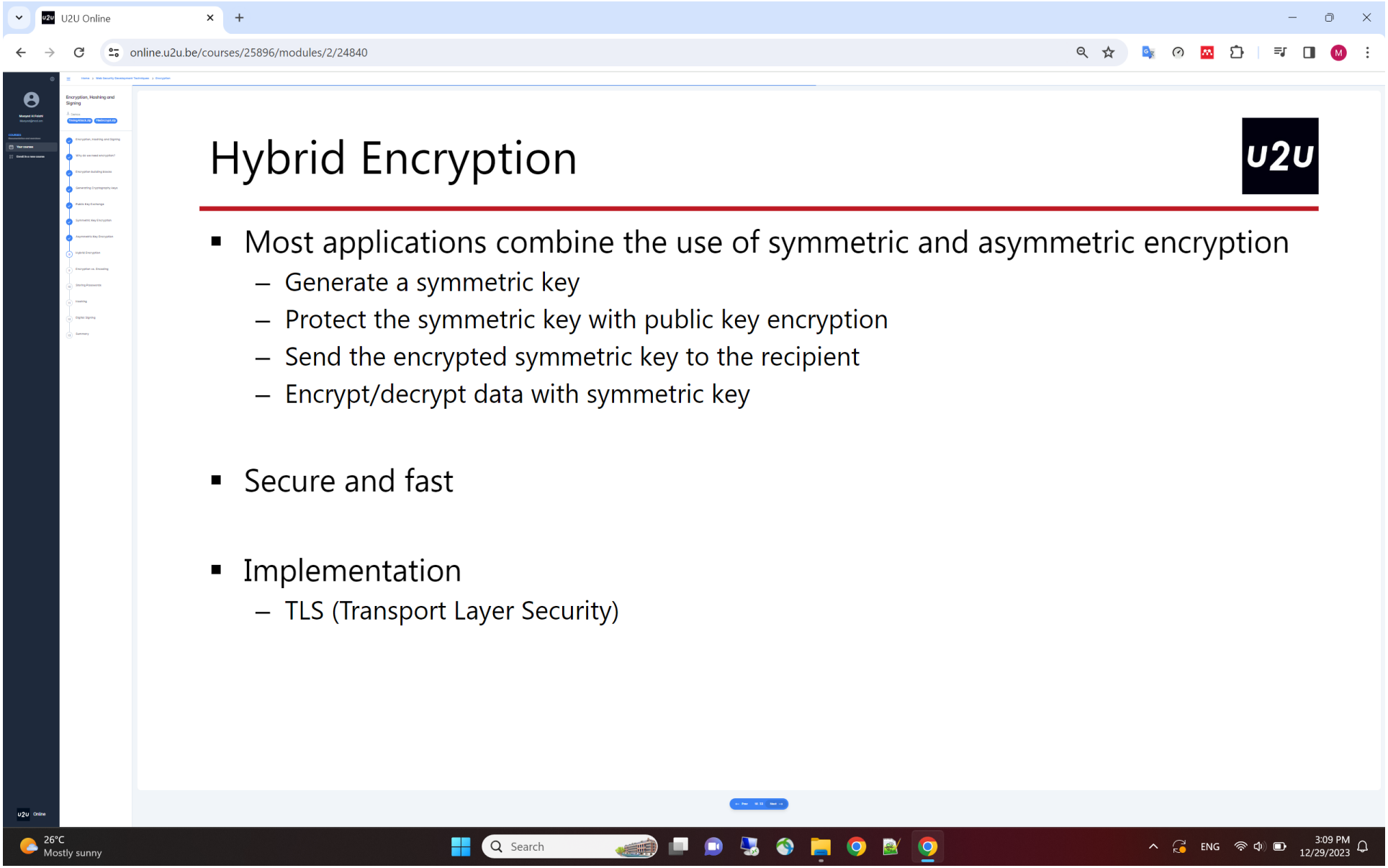

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Symmetric Key Encryption
u2u
Alice
(Sender)
Bob
(Recipient)
Bob and Alice
share the same key
Shared key
Shared key
Cypher text
TXT
Encryption
Decryption
TXT
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023

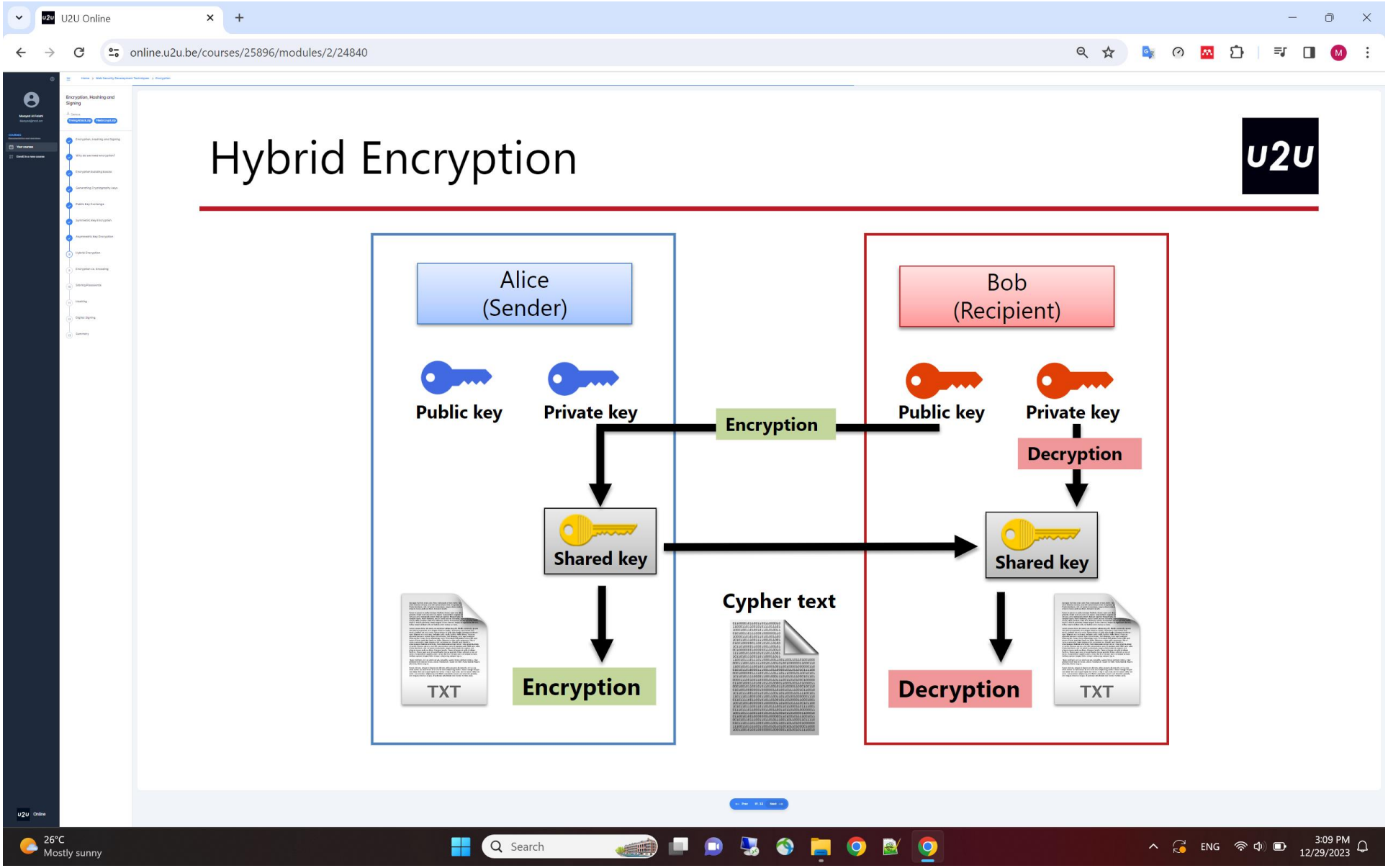

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Symmetric Key Implementations
U2U
Symmetric Key Algorithms
Popular algorithms: Twofish, Serpent, Rijndael, Blowfish, RC4, ...
Standardized algorithm: AES (Advanced Encryption Standard – aka Rijndael)
In .NET use the Aes class
When to use it
Encrypting a bigger stream of data
Encrypting communication between two parties when the key is securily agreed upon
Notable algorithms during history
ROT13 (rotate by 13 places, special form of Caesar cypher)
ENIGMA
DES
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
Asymmetric Key Encryption
U2U
Key pair (mathematically related)
Public key
Available to anyone
Private key
Secret, only you know it
Impossible to derive one key from the other
Encrypt with public key, decrypt with corresponding private key
Pro:
More secure
Con:
Slower
Requires more processing power
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
Asymmetric Key Encryption
U2U
Alice
(Sender)
Private key
Public key
Public key
Bob
TXT
Encryption
Cypher text
Bob
(Recipient)
Private key
Public key
Decryption
TXT
26°C
Mostly sunny
Search
ENG
3:08 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
Asymmetric Key Implementations
U2U
Asymmetric Key Algorithms
Diffie Hellman, RSA, EIGamal,...
Most known: RSA
In .NET use the RSACryptoServiceProvider class
Protocols
PGP (Pretty Good Privacy) or GPG (Gnu Privacy Guard)
Bitcoin
SSH
IKE (Internet Key Exchange, for IPSec)
Use this for sending small messages like communicating a shared key
26°C
Mostly sunny
Search
ENG
3:09 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
Hybrid Encryption
u2u
Most applications combine the use of symmetric and asymmetric encryption
Generate a symmetric key
Protect the symmetric key with public key encryption
Send the encrypted symmetric key to the recipient
Encrypt/decrypt data with symmetric key
Secure and fast
Implementation
TLS (Transport Layer Security)
26°C
Mostly sunny
Search
ENG
3:09 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
Hybrid Encryption
u2u
Alice
(Sender)
Bob
(Recipient)
Public key
Private key
Encryption
Public key
Private key
Decryption
Shared key
Shared key
Cypher text
TXT
Encryption
Decryption
TXT
26°C
Mostly sunny
Search
ENG
3:09 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/2/24840

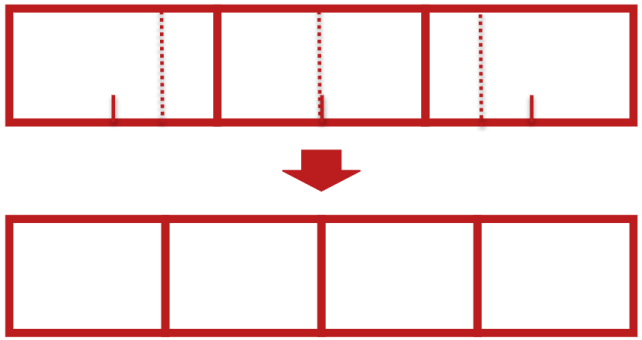
Encryption vs. Encoding

- Encoding != Encryption
- For example: ROT

```
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
```

```
MNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzABCDEFGHIJKL
```

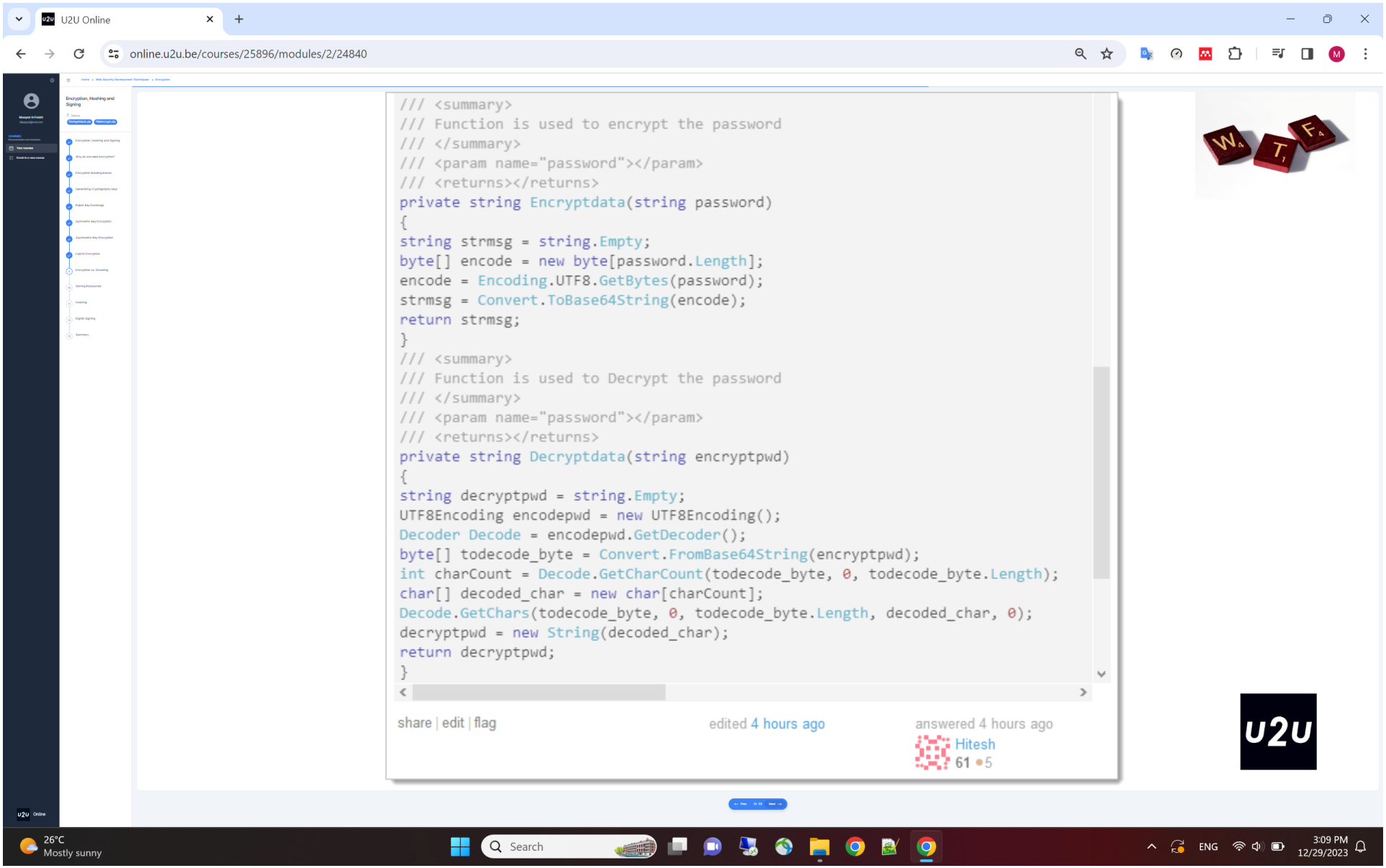
- Base64 Encoding

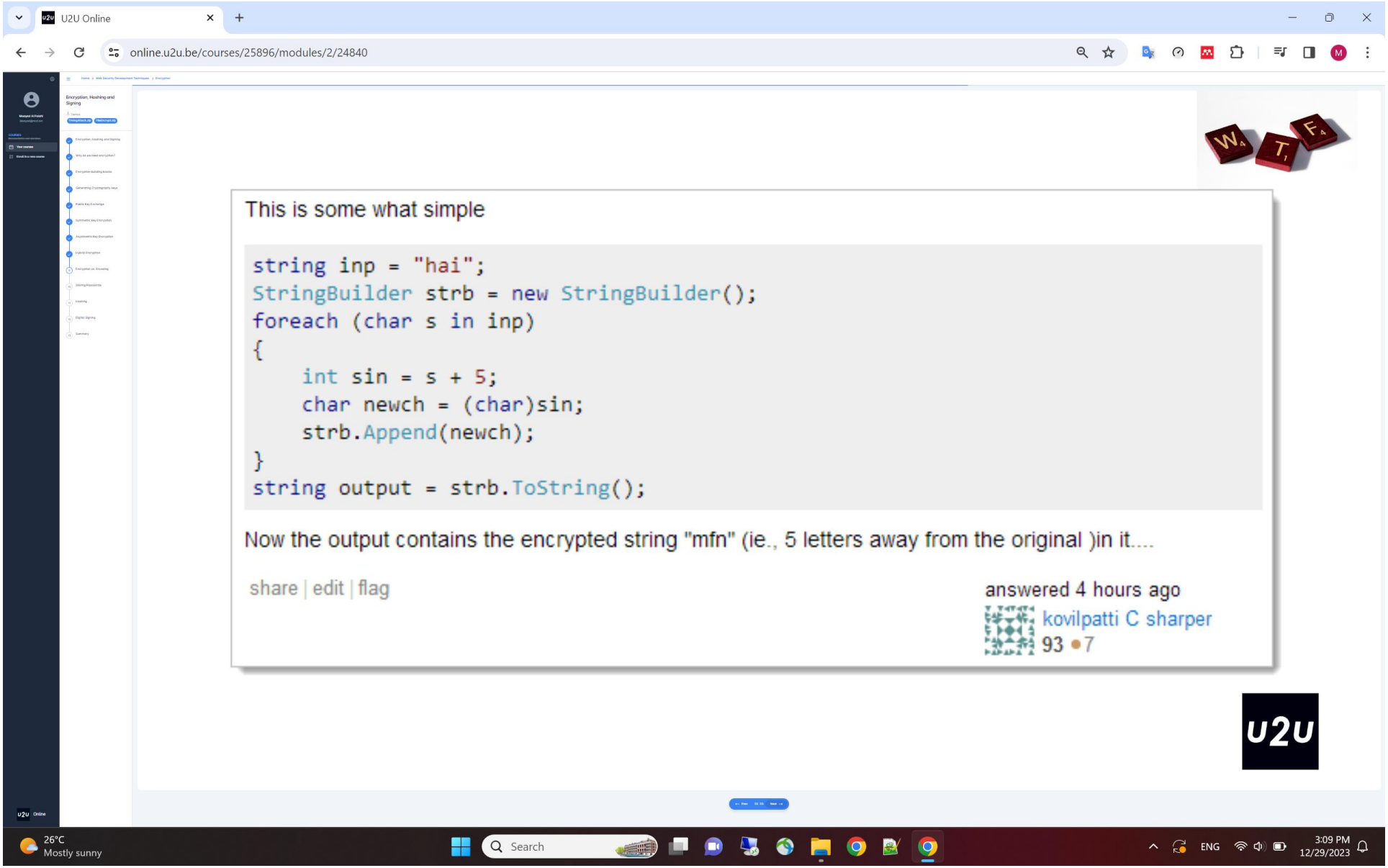


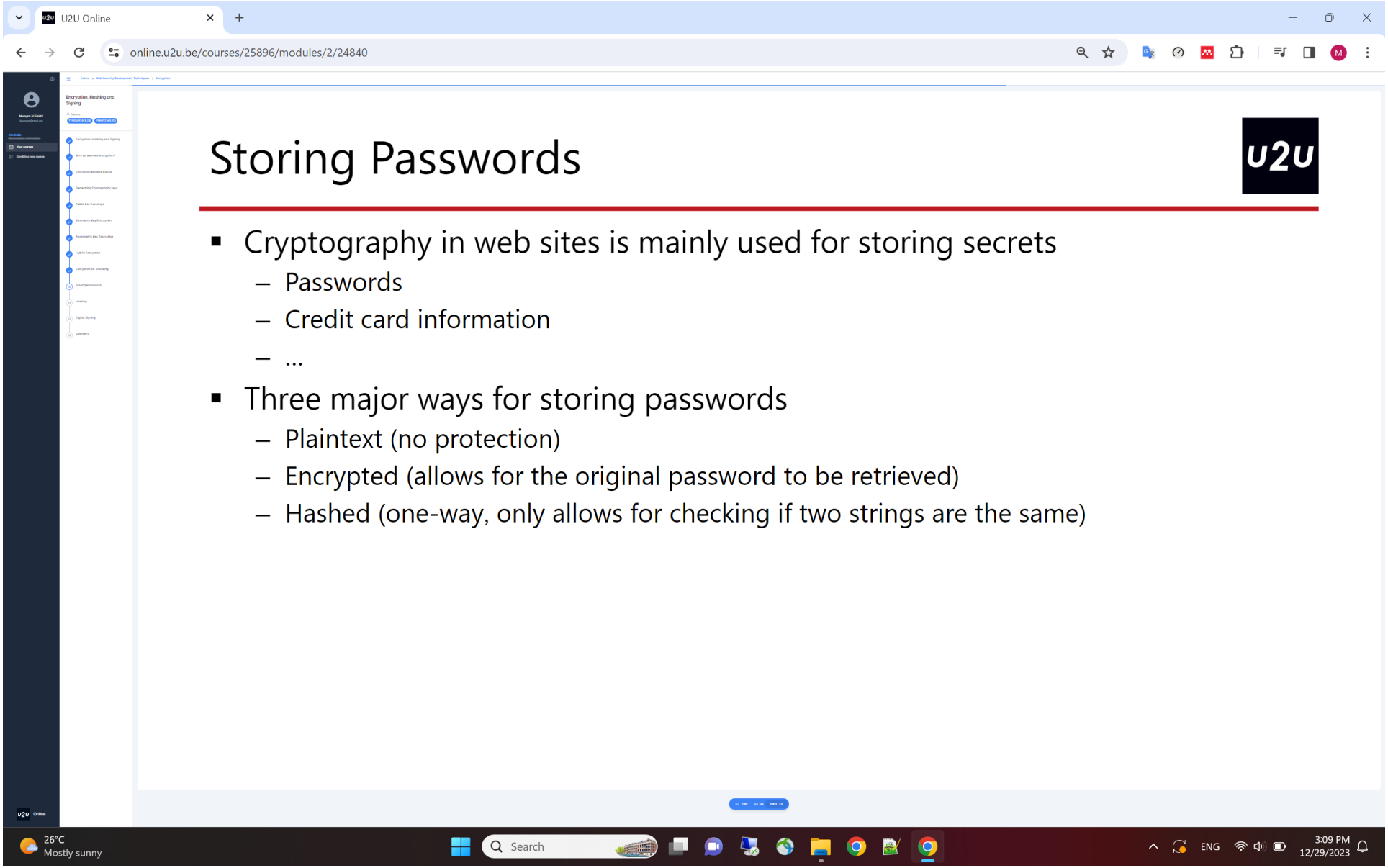
26°C Mostly sunny

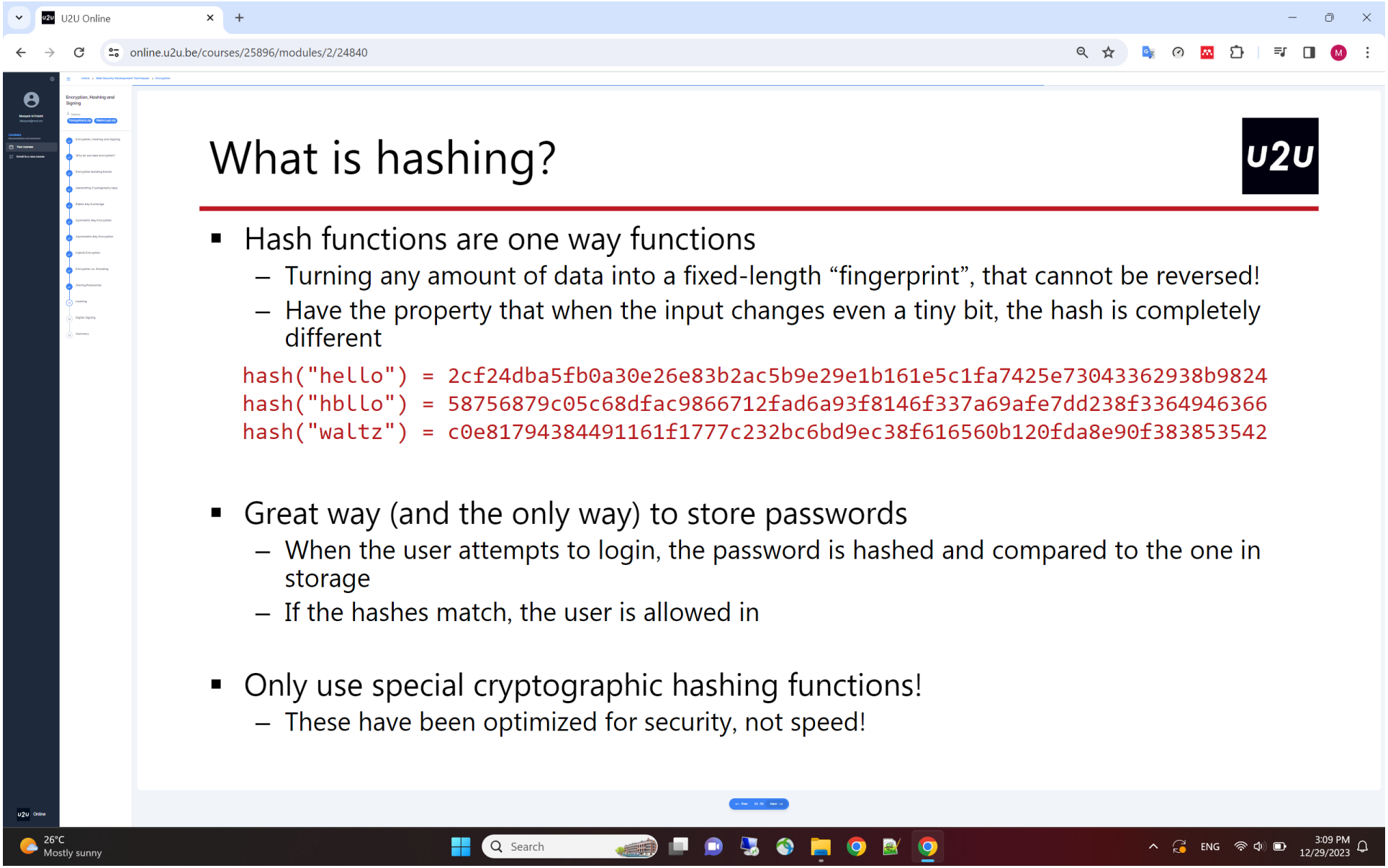
Search

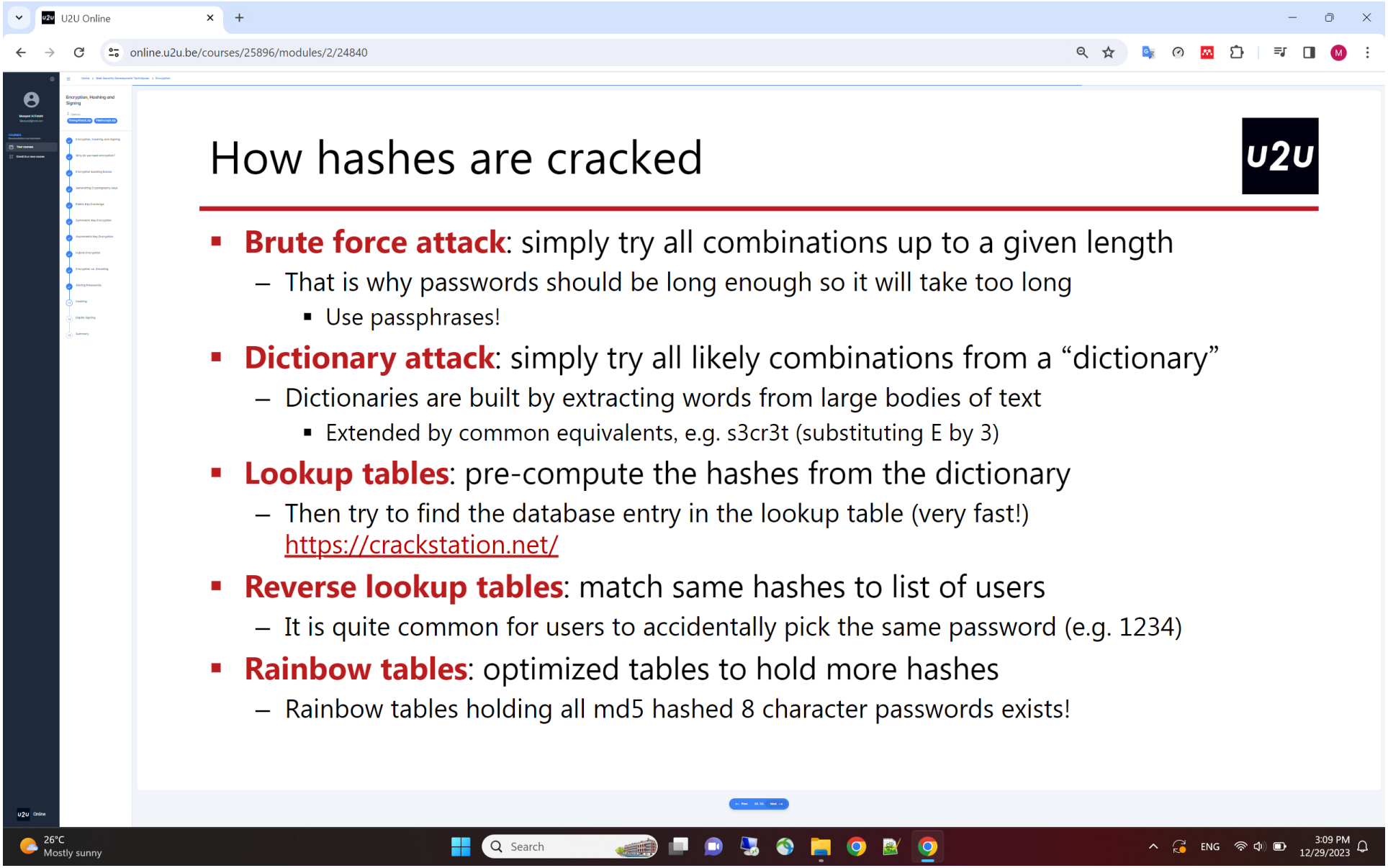
ENG 3:09 PM 12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
/// <summary>
/// Function is used to encrypt the password
/// </summary>
/// <param name="password"></param>
/// <returns></returns>
private string Encryptdata(string password)
{
string strmsg = string.Empty;
byte[] encode = new byte[password.Length];
encode = Encoding.UTF8.GetBytes(password);
strmsg = Convert.ToBase64String(encode);
return strmsg;
}
/// <summary>
/// Function is used to Decrypt the password
/// </summary>
/// <param name="password"></param>
/// <returns></returns>
private string Decryptdata(string encryptpwd)
{
string decryptpwd = string.Empty;
UTF8Encoding encodepwd = new UTF8Encoding();
Decoder Decode = encodepwd.GetDecoder();
byte[] todecode_byte = Convert.FromBase64String(encryptpwd);
int charCount = Decode.GetCharCount(todecode_byte, 0, todecode_byte.Length);
char[] decoded_char = new char[charCount];
Decode.GetChars(todecode_byte, 0, todecode_byte.Length, decoded_char, 0);
decryptpwd = new String(decoded_char);
return decryptpwd;
}
share | edit | flag
edited 4 hours ago
answered 4 hours ago
Hitesh
61 5
u2u
26°C
Mostly sunny
Search
ENG
3:09 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
This is some what simple
string inp = "hai";
StringBuilder strb = new StringBuilder();
foreach (char s in inp)
{
int sin = s + 5;
char newch = (char)sin;
strb.Append(newch);
}
string output = strb.ToString();
Now the output contains the encrypted string "mfn" (ie., 5 letters away from the original)in it....
share | edit | flag
answered 4 hours ago
kovilpatti C sharper
93 • 7
u2u
26°C
Mostly sunny
Search
ENG
3:09 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
Storing Passwords
u2u
Cryptography in web sites is mainly used for storing secrets
Passwords
Credit card information
...
Three major ways for storing passwords
Plaintext (no protection)
Encrypted (allows for the original password to be retrieved)
Hashed (one-way, only allows for checking if two strings are the same)
26°C
Mostly sunny
Search
ENG
3:09 PM
12/29/2023

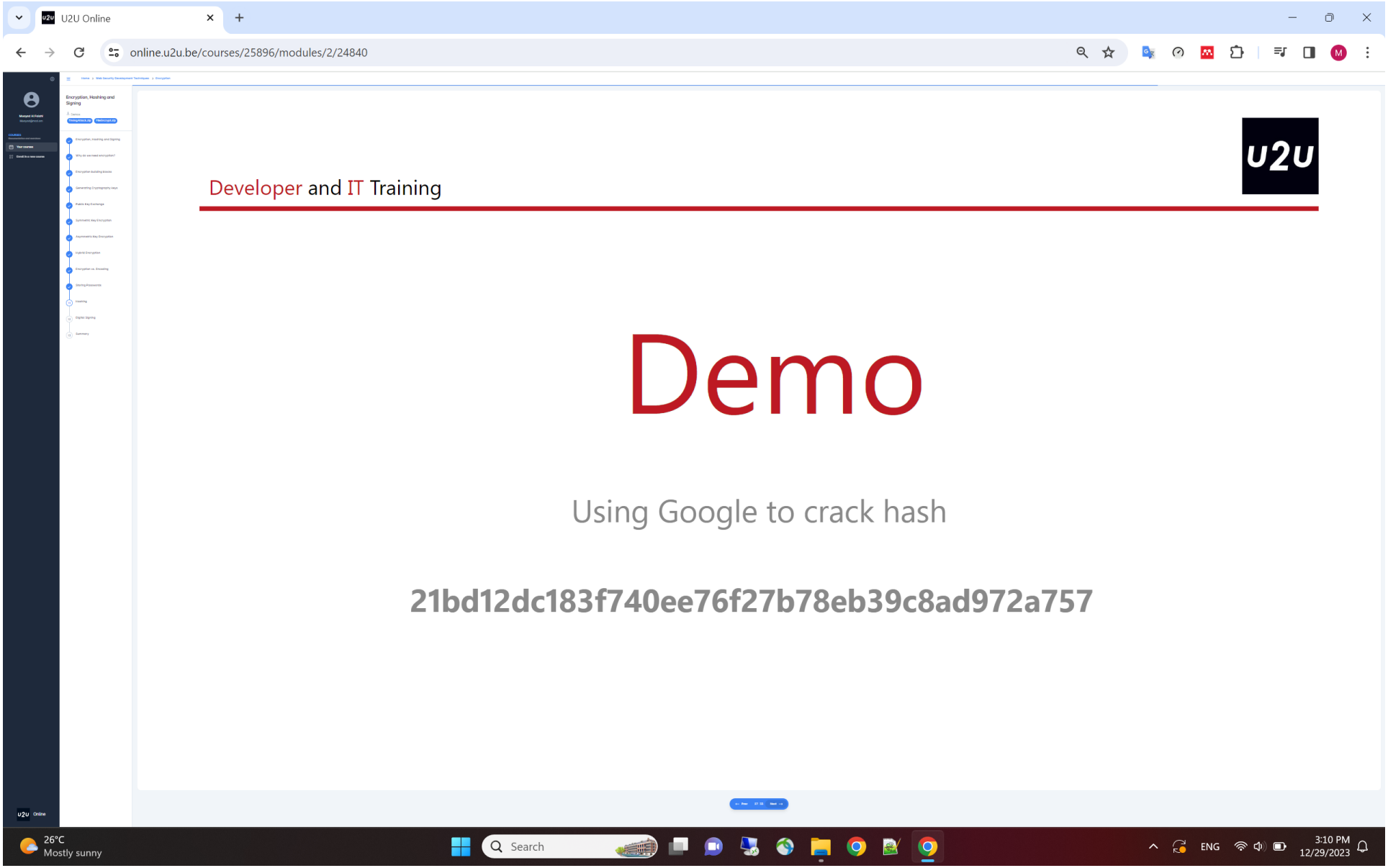

U2U Online
online.u2u.be/courses/25896/modules/2/24840
What is hashing?
u2u
Hash functions are one way functions
Turning any amount of data into a fixed-length “fingerprint”, that cannot be reversed!
Have the property that when the input changes even a tiny bit, the hash is completely different
hash("hello") = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
hash("hbllo") = 58756879c05c68dfac9866712fad6a93f8146f337a69afe7dd238f3364946366
hash("waltz") = c0e81794384491161f1777c232bc6bd9ec38f616560b120fda8e90f383853542
Great way (and the only way) to store passwords
When the user attempts to login, the password is hashed and compared to the one in storage
If the hashes match, the user is allowed in
Only use special cryptographic hashing functions!
These have been optimized for security, not speed!
26°C
Mostly sunny
Search
ENG
3:09 PM
12/29/2023

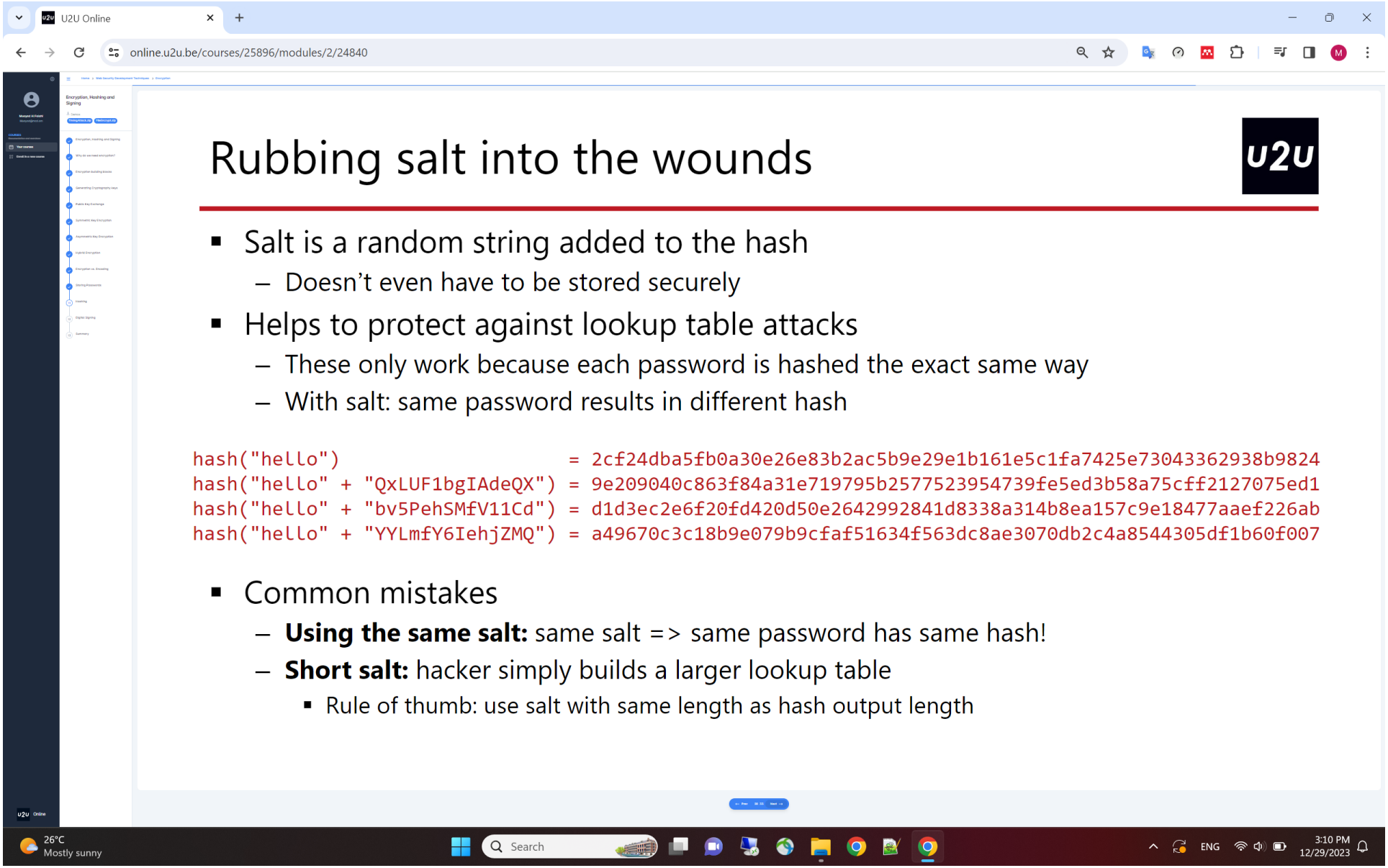

U2U Online
online.u2u.be/courses/25896/modules/2/24840
How hashes are cracked
U2U
Brute force attack: simply try all combinations up to a given length
That is why passwords should be long enough so it will take too long
Use passphrases!
Dictionary attack: simply try all likely combinations from a “dictionary”
Dictionaries are built by extracting words from large bodies of text
Extended by common equivalents, e.g. s3cr3t (substituting E by 3)
Lookup tables: pre-compute the hashes from the dictionary
Then try to find the database entry in the lookup table (very fast!)
https://crackstation.net/
Reverse lookup tables: match same hashes to list of users
It is quite common for users to accidentally pick the same password (e.g. 1234)
Rainbow tables: optimized tables to hold more hashes
Rainbow tables holding all md5 hashed 8 character passwords exists!
26°C
Mostly sunny
Search
ENG
3:09 PM
12/29/2023

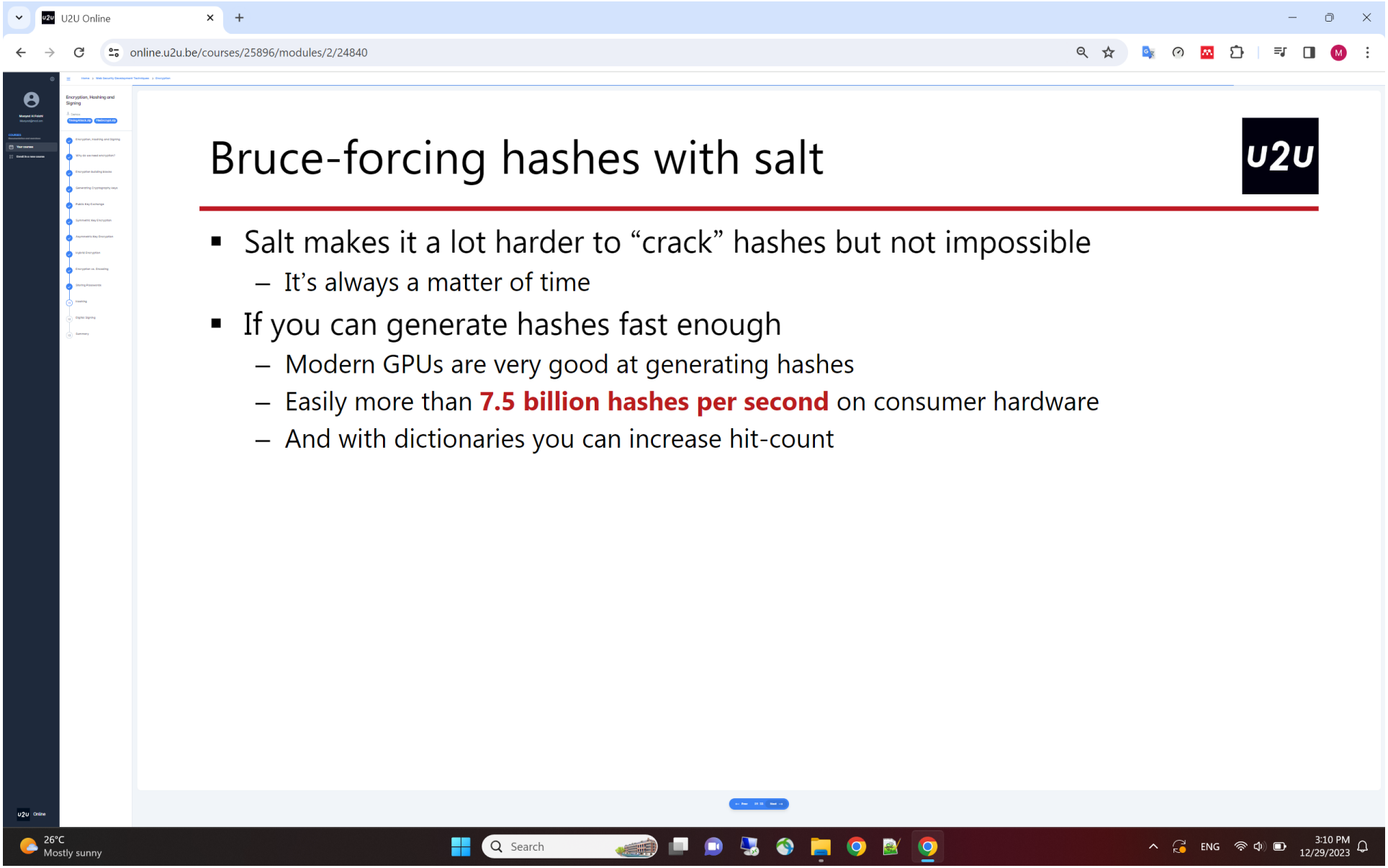
Typical Cracking Hardware

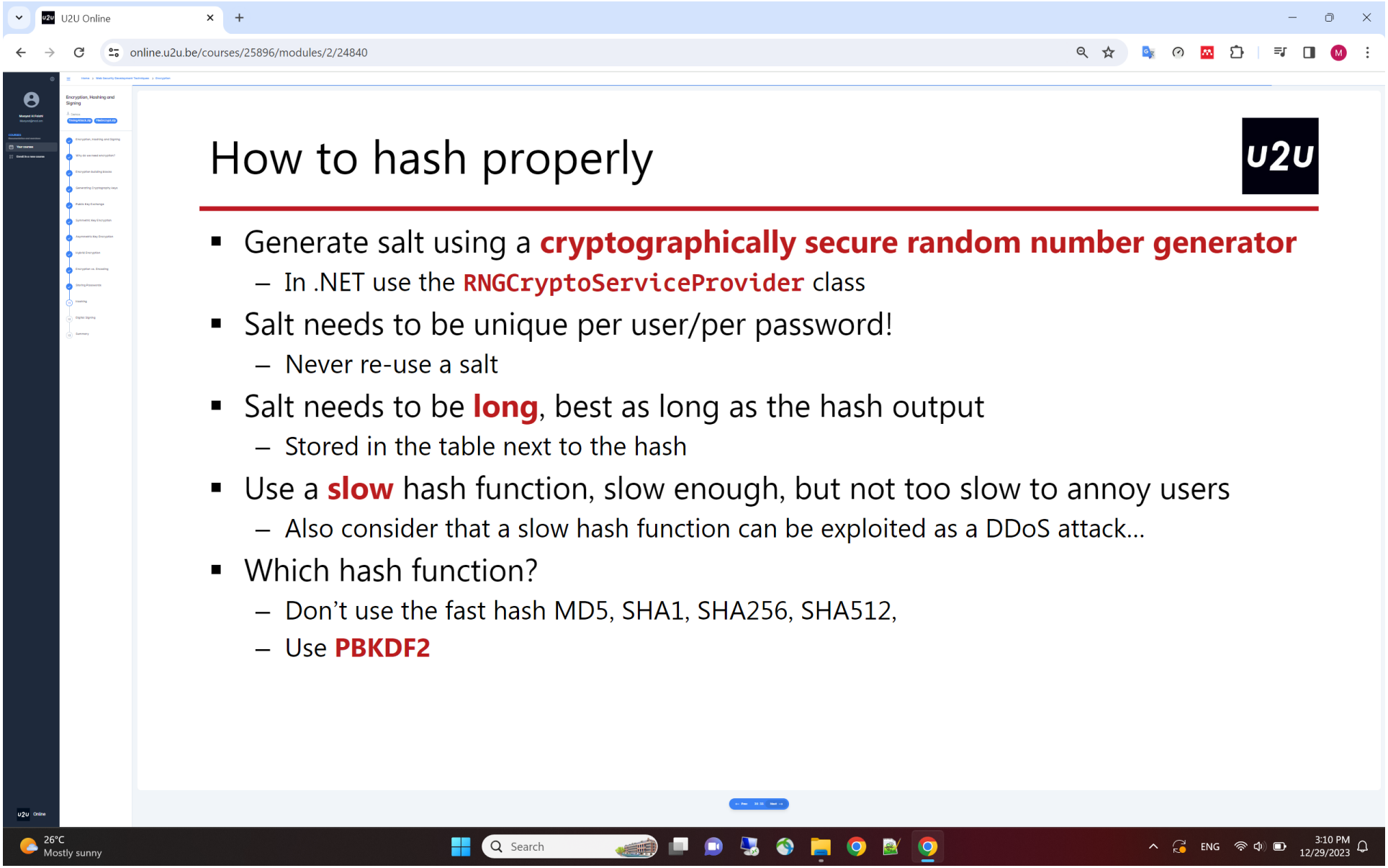
- Lots of GPUs
- Google
  - Hashcat performance

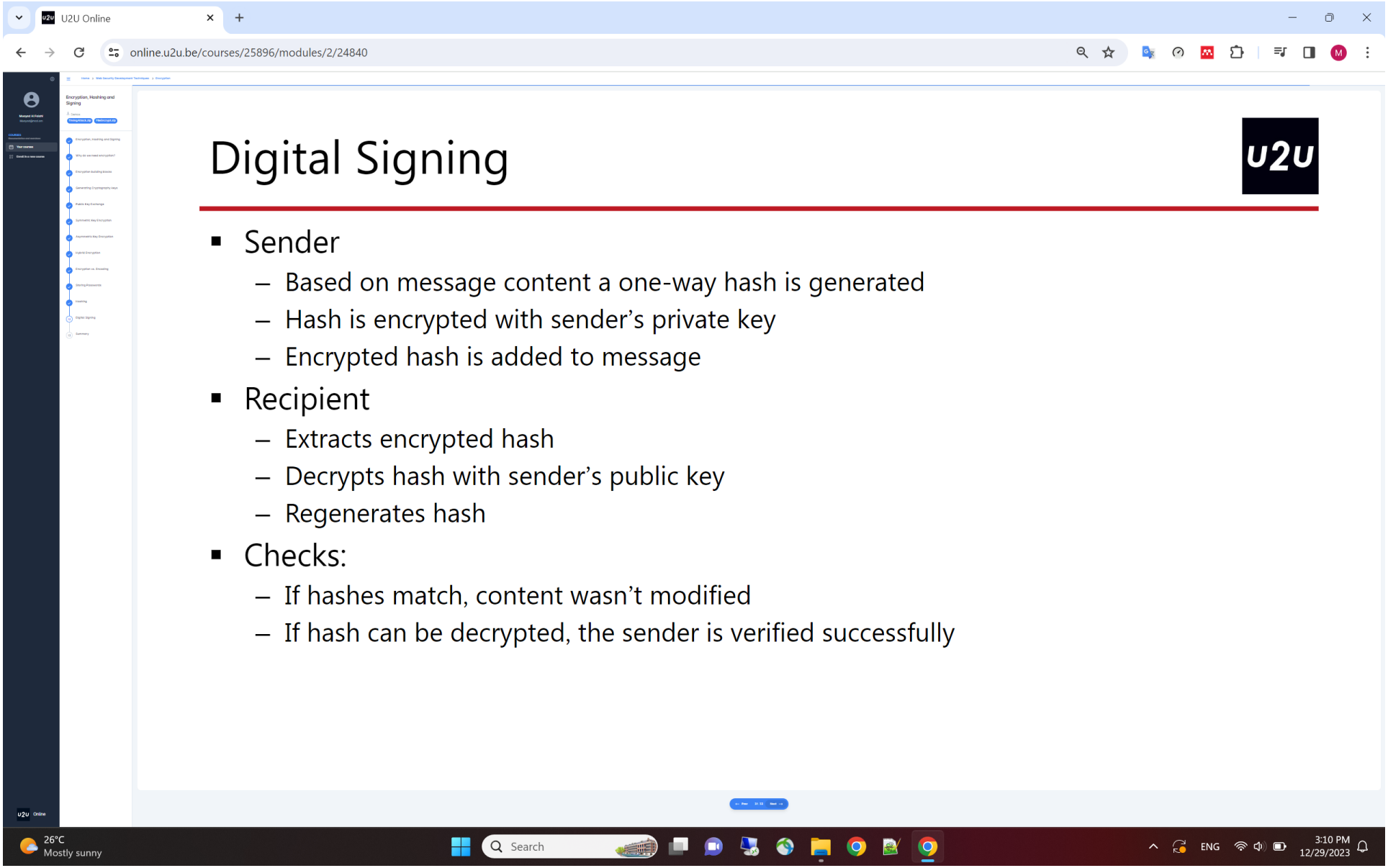
http://thepasswordproject.com/oclhashcat_benchmarking

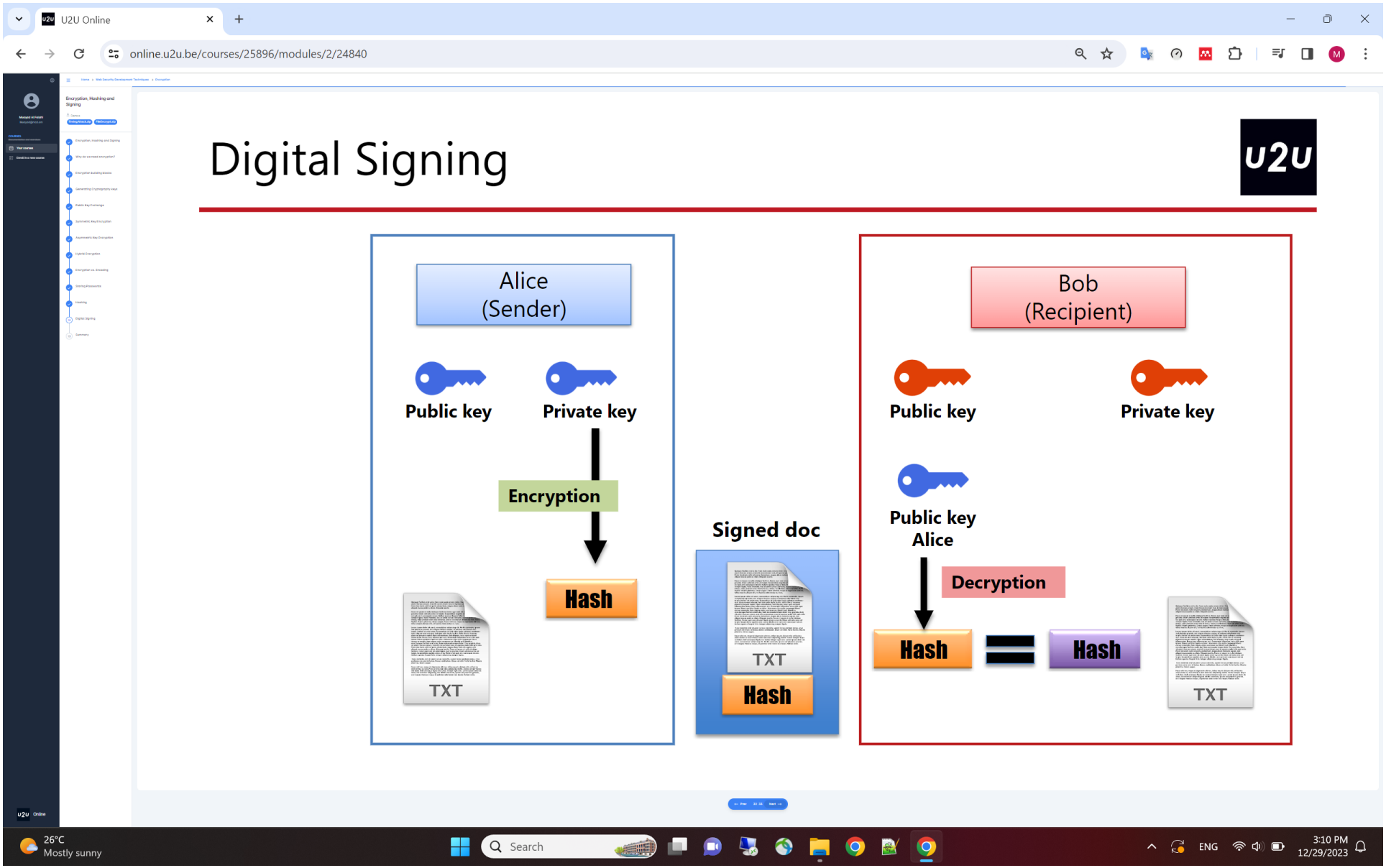

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Developer and IT Training
U2U
Demo
Using Google to crack hash
21bd12dc183f740ee76f27b78eb39c8ad972a757
26°C
Mostly sunny
Search
ENG
3:10 PM
12/29/2023

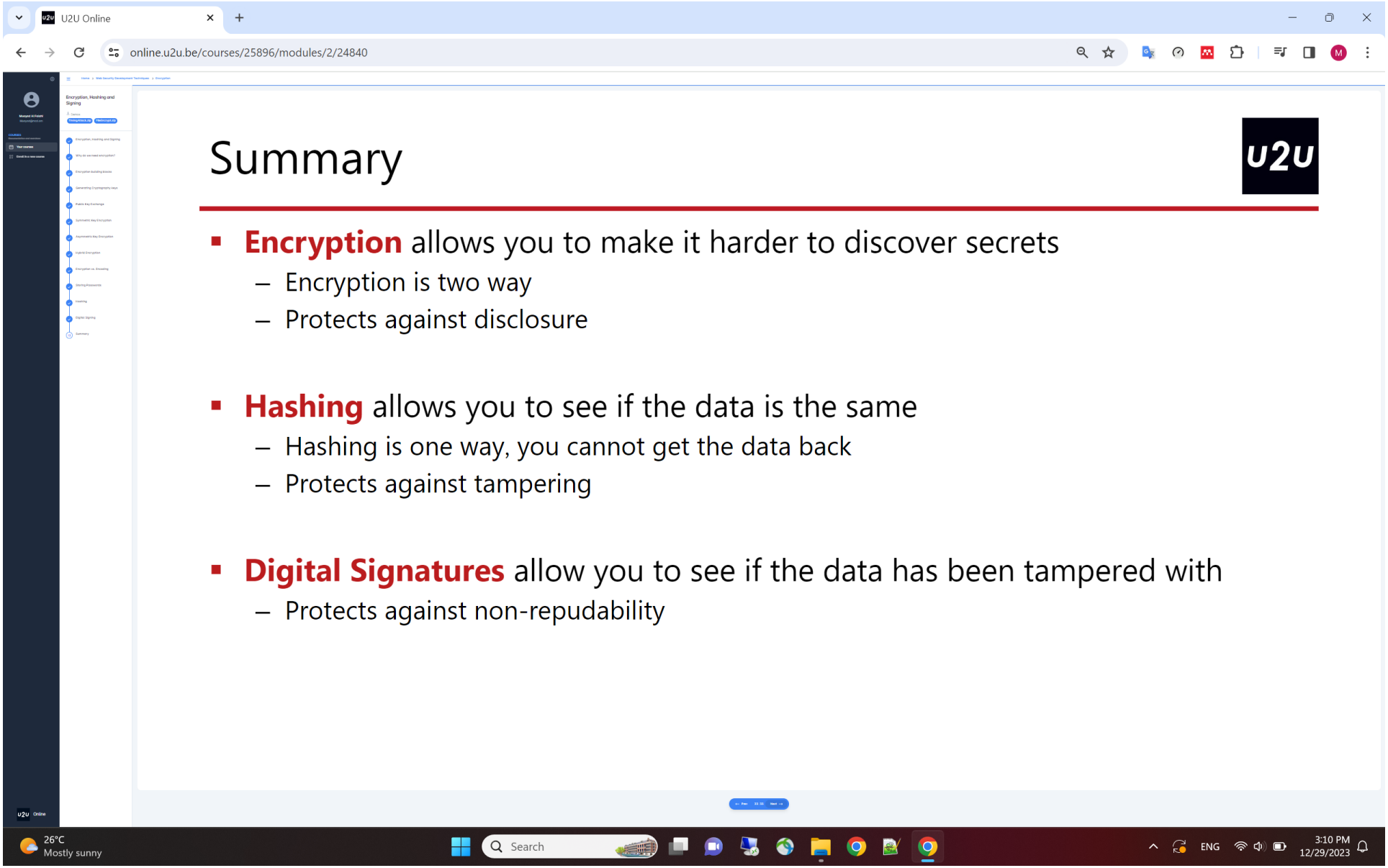

U2U Online
online.u2u.be/courses/25896/modules/2/24840
Rubbing salt into the wounds
U2U
Salt is a random string added to the hash
Doesn't even have to be stored securely
Helps to protect against lookup table attacks
These only work because each password is hashed the exact same way
With salt: same password results in different hash
hash("hello") = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
hash("hello" + "QxLUF1bgIAdeQX") = 9e209040c863f84a31e719795b2577523954739fe5ed3b58a75cff2127075ed1
hash("hello" + "bv5PehSMfV11Cd") = d1d3ec2e6f20fd420d50e2642992841d8338a314b8ea157c9e18477aaef226ab
hash("hello" + "YYLmfY6IehjZMQ") = a49670c3c18b9e079b9cfaf51634f563dc8ae3070db2c4a8544305df1b60f007
Common mistakes
Using the same salt: same salt => same password has same hash!
Short salt: hacker simply builds a larger lookup table
Rule of thumb: use salt with same length as hash output length
26°C
Mostly sunny
Search
ENG
3:10 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
Bruce-forcing hashes with salt
U2U
Salt makes it a lot harder to “crack” hashes but not impossible
It’s always a matter of time
If you can generate hashes fast enough
Modern GPUs are very good at generating hashes
Easily more than 7.5 billion hashes per second on consumer hardware
And with dictionaries you can increase hit-count
26°C
Mostly sunny
Search
ENG
3:10 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
How to hash properly
U2U
Generate salt using a cryptographically secure random number generator
In .NET use the RNGCryptoServiceProvider class
Salt needs to be unique per user/per password!
Never re-use a salt
Salt needs to be long, best as long as the hash output
Stored in the table next to the hash
Use a slow hash function, slow enough, but not too slow to annoy users
Also consider that a slow hash function can be exploited as a DDoS attack…
Which hash function?
Don't use the fast hash MD5, SHA1, SHA256, SHA512,
Use PBKDF2
26°C
Mostly sunny
Search
ENG
3:10 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
Digital Signing
u2u
Sender
Based on message content a one-way hash is generated
Hash is encrypted with sender's private key
Encrypted hash is added to message
Recipient
Extracts encrypted hash
Decrypts hash with sender's public key
Regenerates hash
Checks:
If hashes match, content wasn't modified
If hash can be decrypted, the sender is verified successfully
26°C
Mostly sunny
Search
ENG
3:10 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
Digital Signing
u2u
Alice
(Sender)
Public key
Private key
Encryption
Hash
TXT
Signed doc
TXT
Hash
Bob
(Recipient)
Public key
Private key
Public key
Alice
Decryption
Hash
Hash
TXT
26°C
Mostly sunny
Search
ENG
3:10 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/2/24840
Summary
u2u
Encryption allows you to make it harder to discover secrets
Encryption is two way
Protects against disclosure
Hashing allows you to see if the data is the same
Hashing is one way, you cannot get the data back
Protects against tampering
Digital Signatures allow you to see if the data has been tampered with
Protects against non-repudability
26°C
Mostly sunny
Search
ENG
3:10 PM
12/29/2023