

ОСНОВИ КІБЕРГІЄНИ

**Безпечне користування електронною
ПОШТОЮ**

Цілі

- налаштувати двофакторну автентифікацію
- опанувати використання парольного менеджера
- впровадити використання електронного підпису та шифрування повідомлень*

Що таке E-Mail?



<https://www.youtube.com/watch?v=VEYC1VnnEaY>

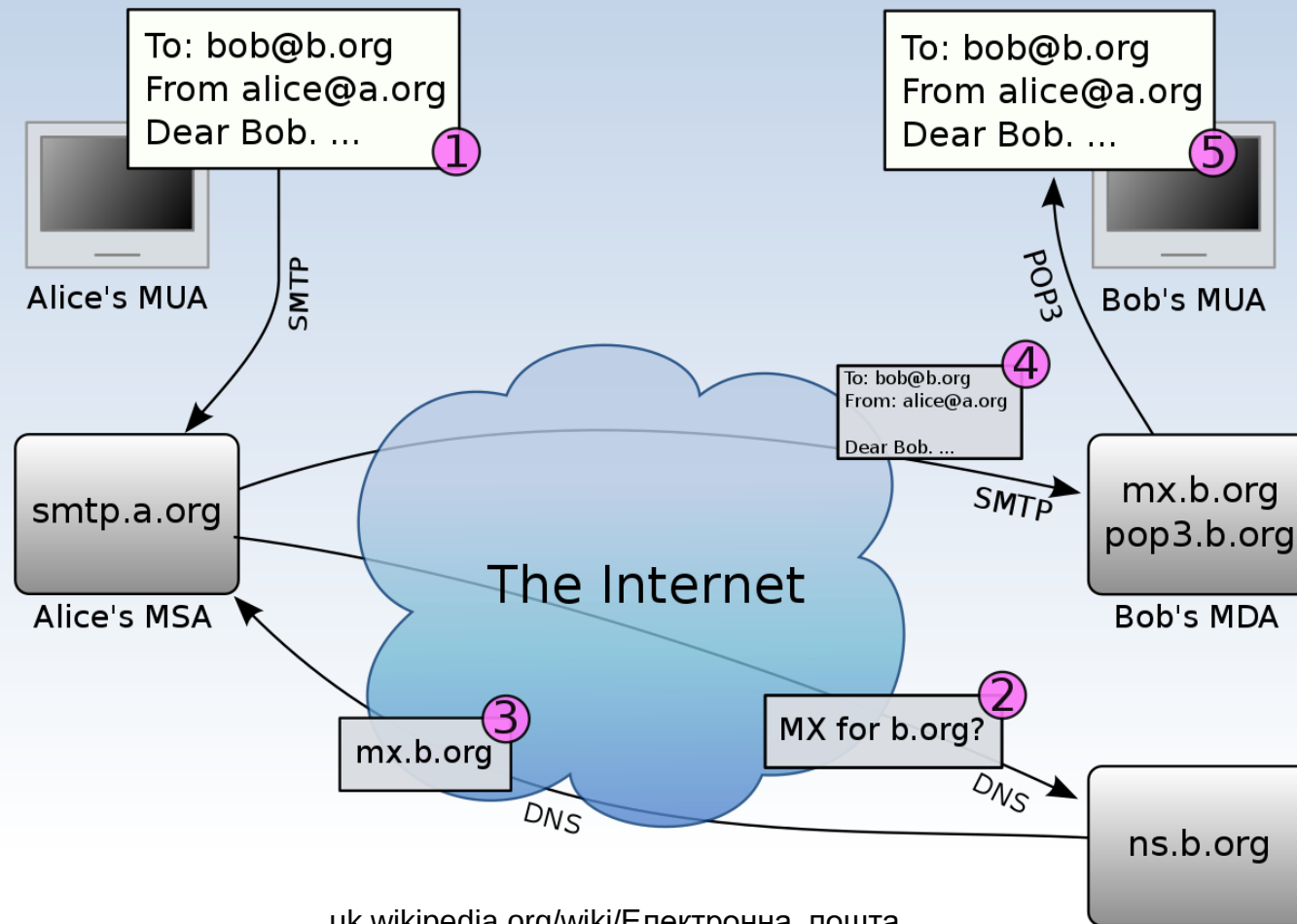


Організація з безпеки та співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

Що таке E-Mail?



uk.wikipedia.org/wiki/Електронна_пошта

Що таке E-Mail?



<https://www.youtube.com/watch?v=VEYC1VnnEaY>

Від яких кіберзагроз будемо вчитися захищатися?

- крадіжка паролю
- вгадування (підбір) «простого» паролю зловмисником для декількох ресурсів користувача
- підробка електронних листів
- порушення конфіденційності листування

Як будемо захищатись?

- додатковий одноразовий пароль
- складні паролі для різних ресурсів і безпечне їх зберігання
- електронний підпис повідомлень
- шифрування листування

Як придумати складний пароль, який ви запам'ятаєте?



Організація з безпеки та
співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

Двофакторна автентифікація поштового облікового запису

- Створити безкоштовні особисті поштові облікові записи в доменах gmail.com та protonmail.com.
- Налаштувати двофакторну автентифікацію через Google Authenticator для облікових записів gmail.com та protonmail.com.

Відео
виконання



Організація з безпеки та співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

Парольний менеджер

- Завантажити, встановити та запустити парольний менеджер KeePass Password Safe.
- Опанувати його використання

<https://2ip.io/ua/passcheck/>

Відео
виконання

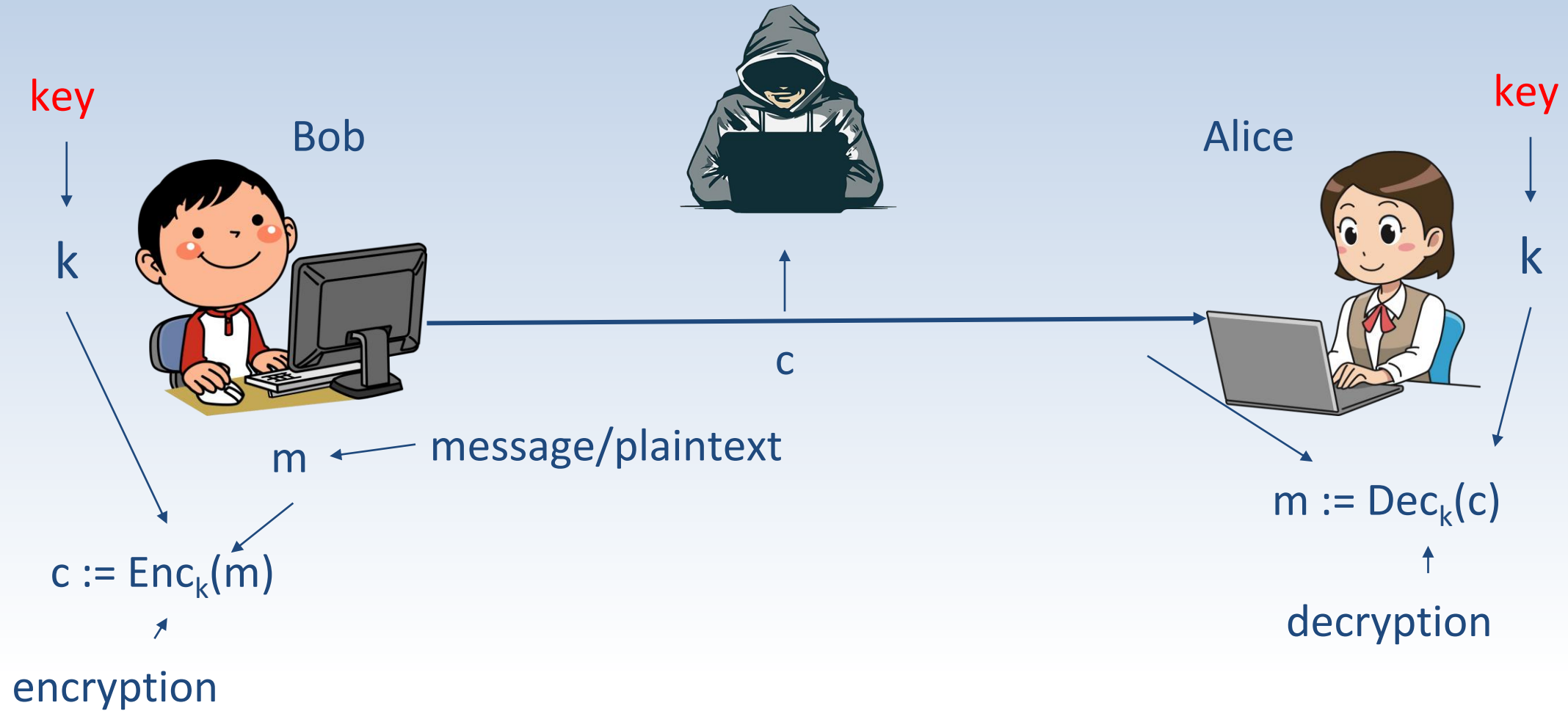


Організація з безпеки та
співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

Криптосистема з приватним ключем

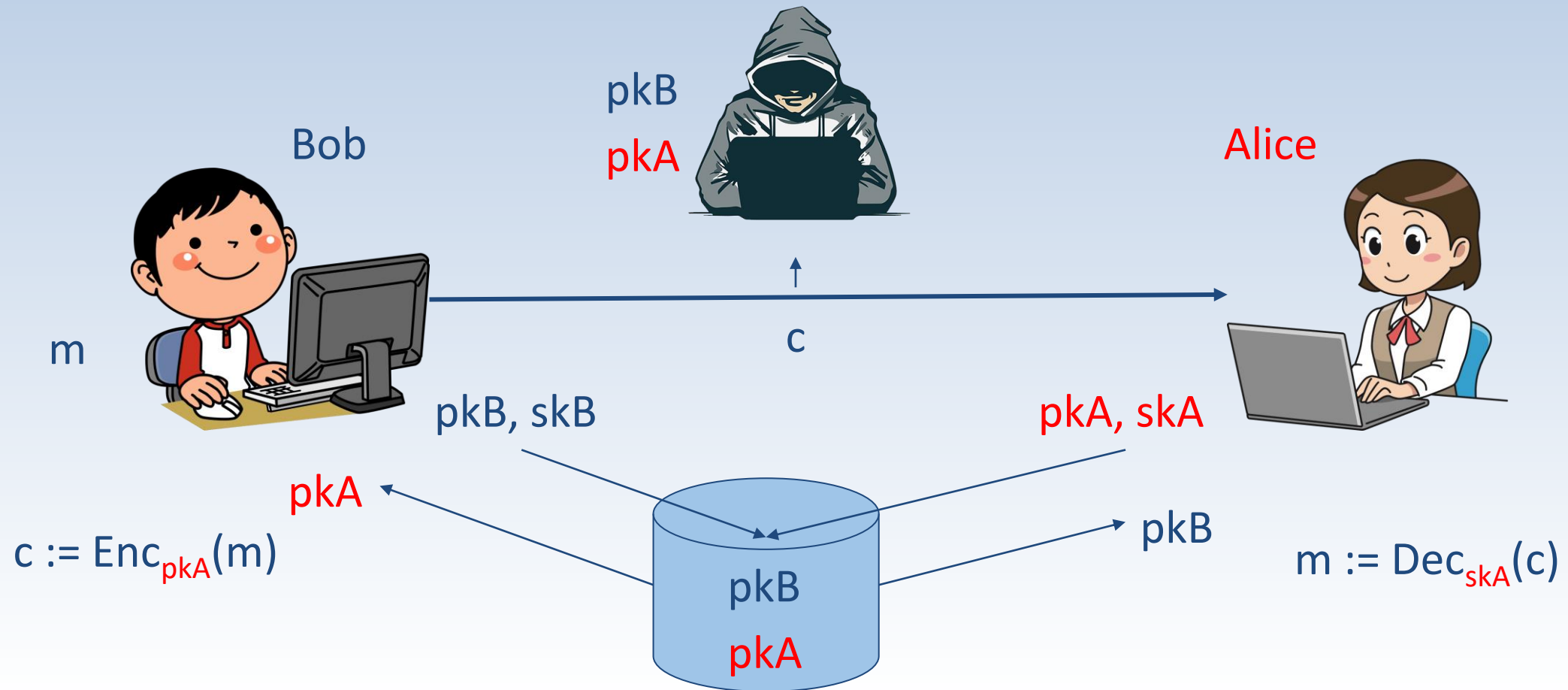


AES String Encryption and Decryption

- cryptotools.net/aes - bit.ly/3oQaHGR



Криптосистема з публічним ключем



Шифрування/розшифрування з публічним ключем

- [шифрування/розшифрування за RSA](https://bit.ly/3kXNr8N) - bit.ly/3kXNr8N



Криптографічна ґеш-функція



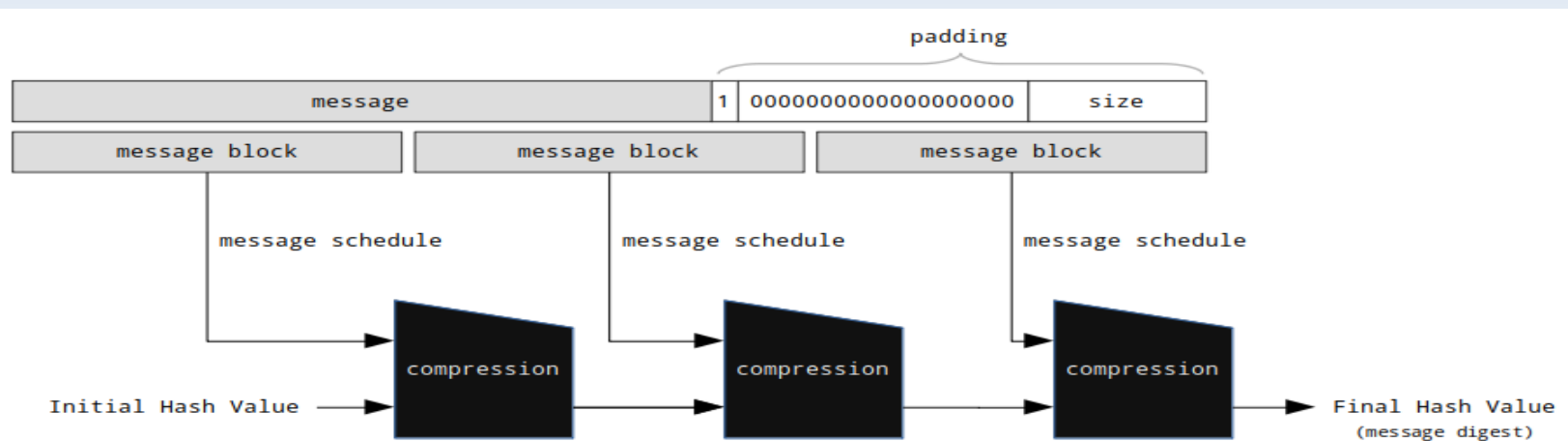
→ $h(x)$ → 14458912610626287058



1. Input Image

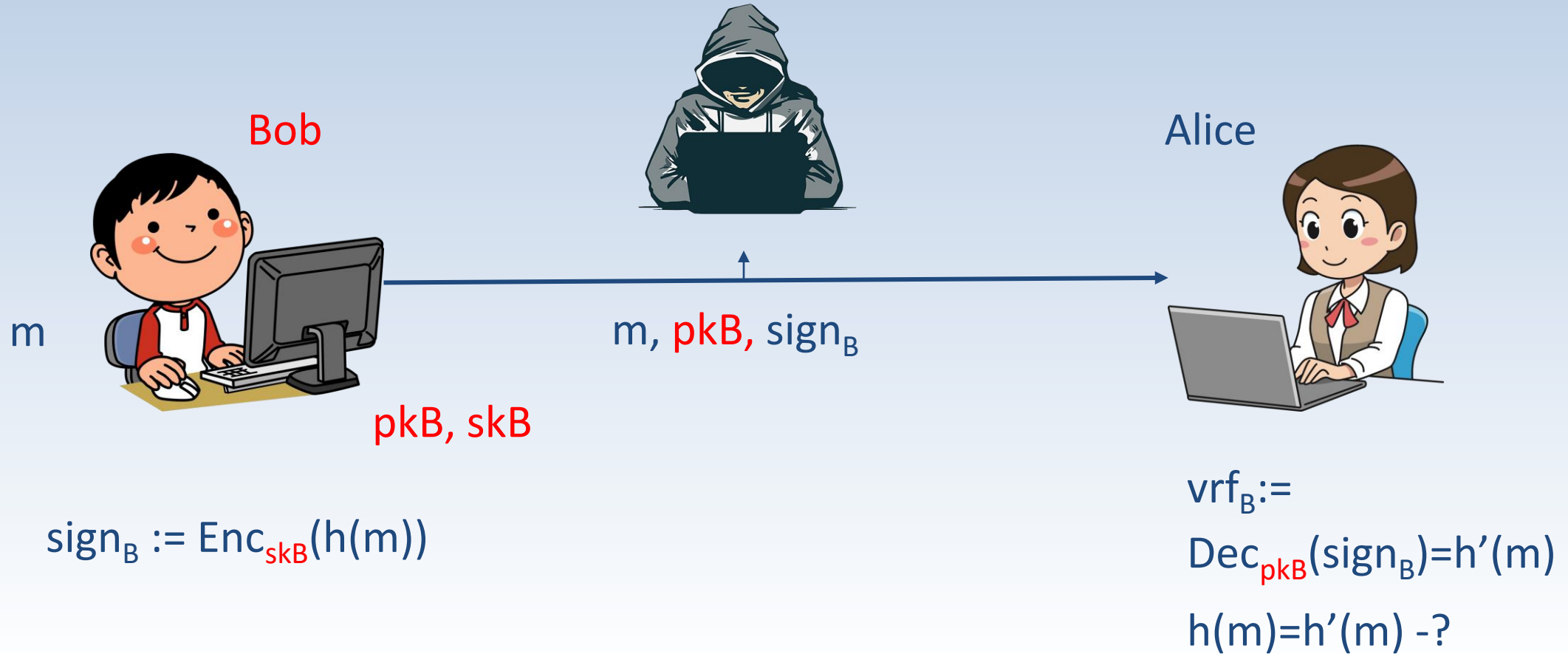
2. Hashing Function

3. Image Fingerprint



<https://awesomeopensource.com/project/in3rsha/sha256-animation>

Електронний підпис та його перевірка



8gwifi.org

Основні відомості про криптосистеми



Електронний підпис та шифрування повідомлень

- утиліта **gpg4usb**
- розширення **FlowCrypt: Encrypt Gmail with PGP**
- вбудований сервіс **ProtonMail**

Відео виконання



Підсумки

- ми навчилися захищатися від:
 - несанкціонованого доступу до поштового облікового запису у випадку крадіжки паролю
 - вгадування «простого» паролю для декількох ресурсів
 - підробки електронних листів
 - порушення конфіденційності листування

