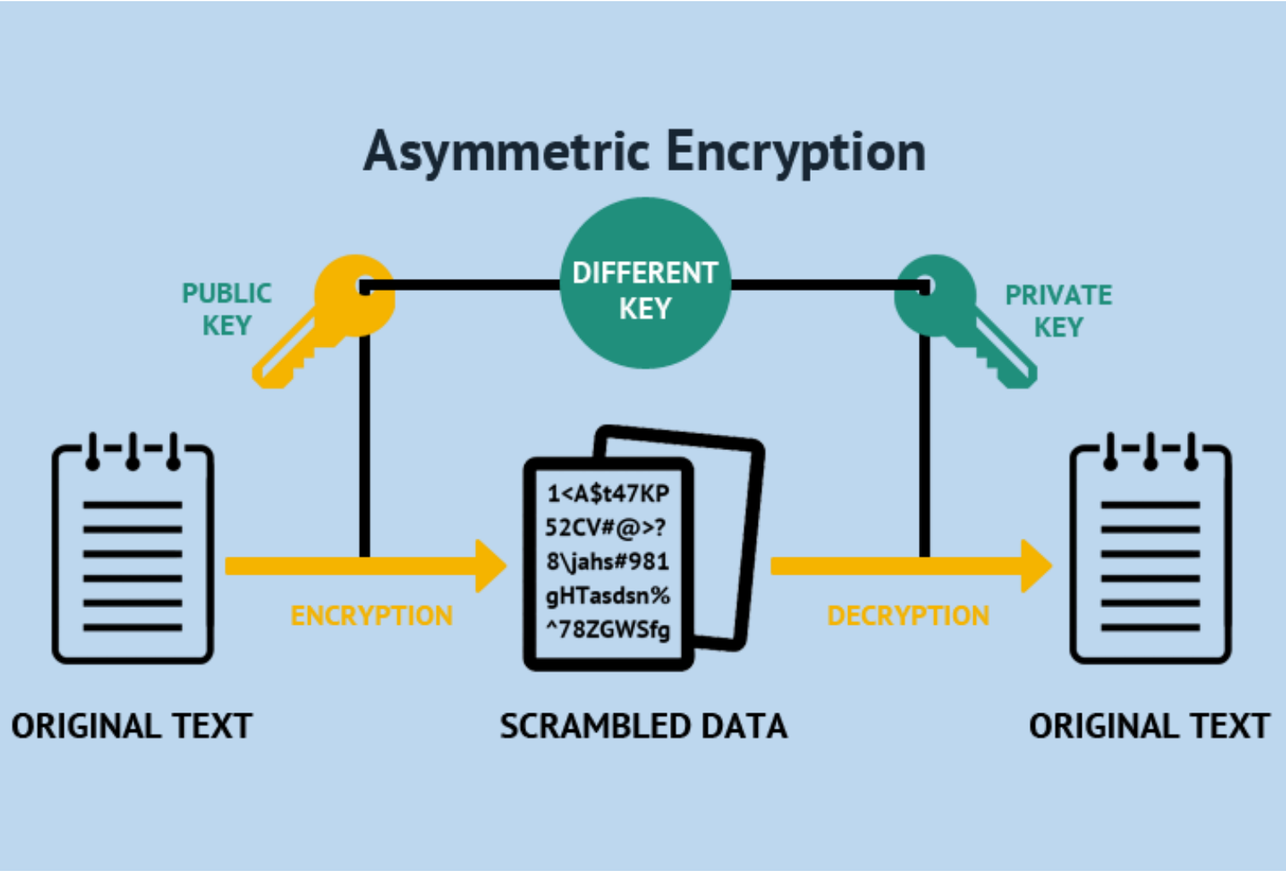
ЛЕКЦІЯ 8

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Основні положення криптографії з відкритим ключем



План

1. Ідея криптосистеми з відкритим ключем
2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)
3. Симетричні шифри vs асиметричні шифри

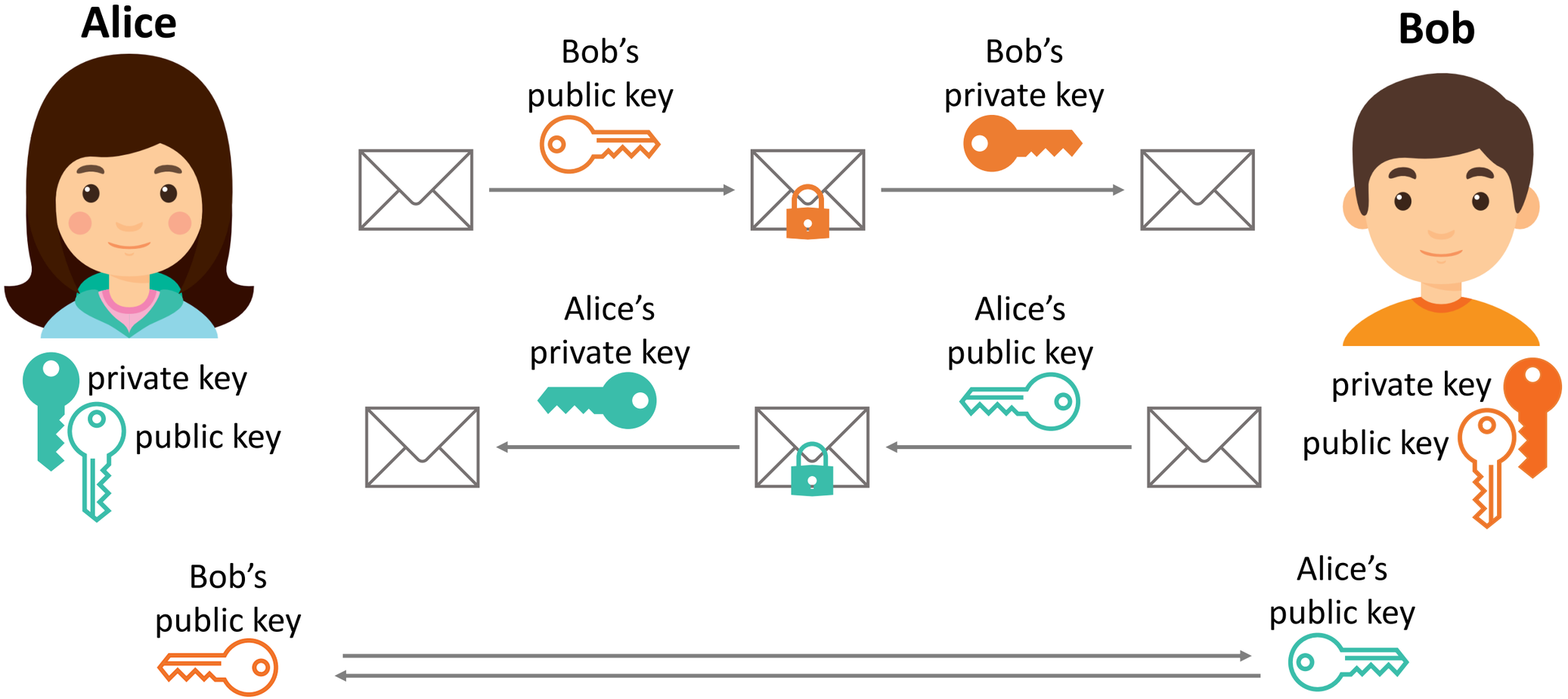
1. Ідея криптосистеми з відкритим ключем

Ідея криптосистеми з відкритим ключем була висунута американськими криптографами Уітфілдом Діффі та Мартіном Хелманом (1976 рік), і окремо Ральфом Мерклом (1978 рік)

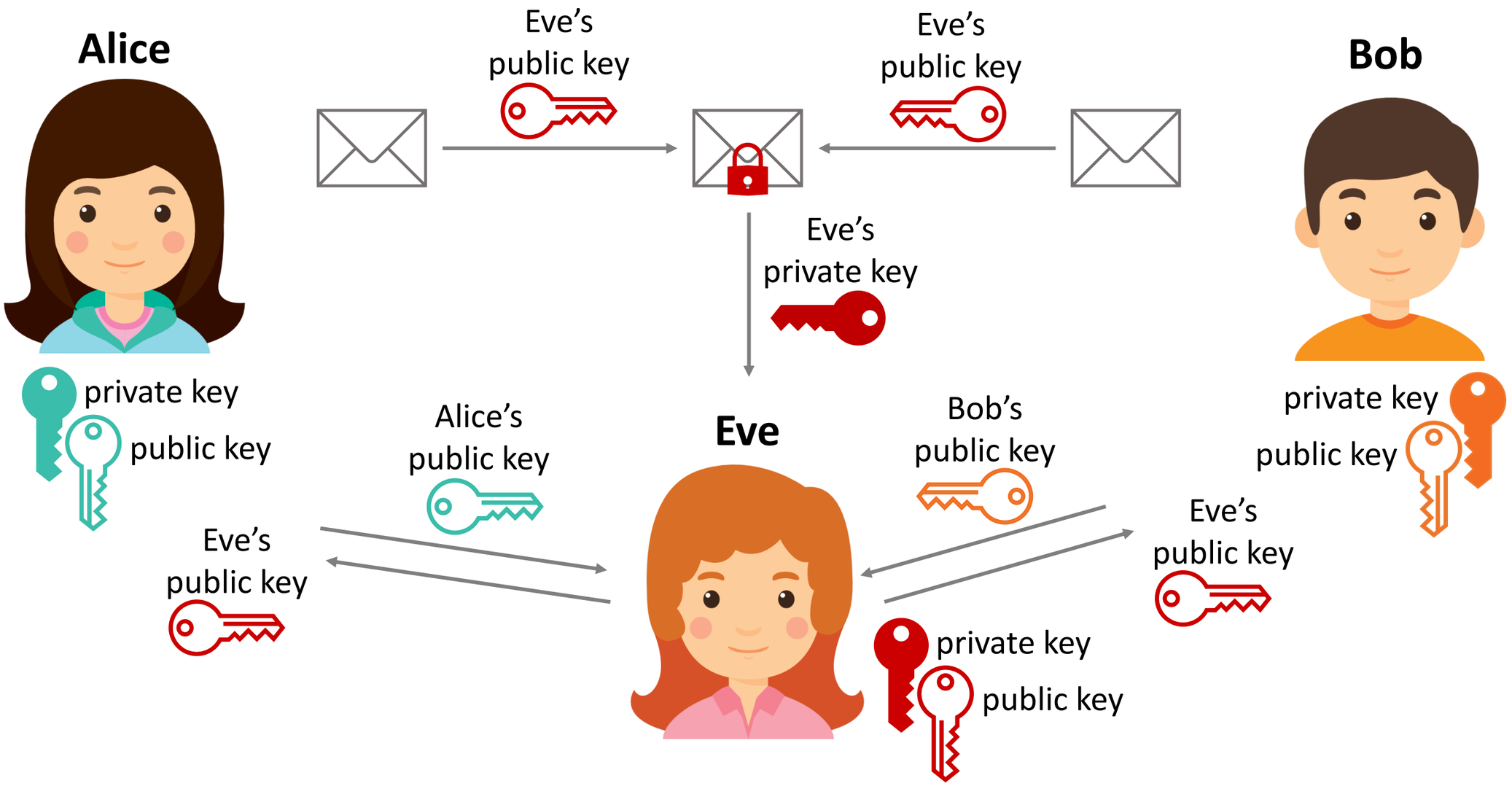
У асиметричних криптосистемах для шифрування використовується відкритий ключ (публічний), а для дешифрування – закритий (приватний)

Ральф Меркл | Мартін Хелман | Уітфілд Діффі

1. Ідея криптосистеми з відкритим ключем



1. Ідея криптосистеми з відкритим ключем



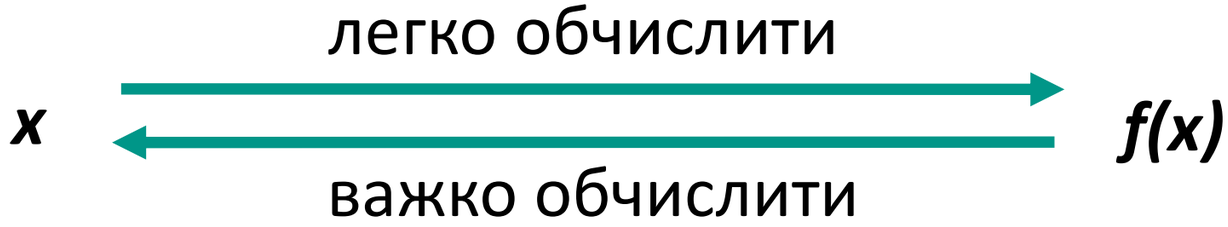
1. Ідея криптосистеми з відкритим ключем

How asymmetric (public key) encryption works

1. Ідея криптосистеми з відкритим ключем

Математична база

Ідея криптографії з відкритим ключем тісно пов'язана з ідеєю однобічних функцій (one-way function), тобто таких функцій *f(x)*, що по відомому *x* досить просто знайти значення *f(x)*, тоді як визначити *x* з *f(x)* важко



1. Ідея криптосистеми з відкритим ключем

Математична база

Також використовуються однобічні функції з лазівкою (one-way trap-door function).

Лазівка – це певний секрет, що допомагає розшифрувати. Тобто існує такий *y*, що знаючи *f(x),* можна обчислити *x*

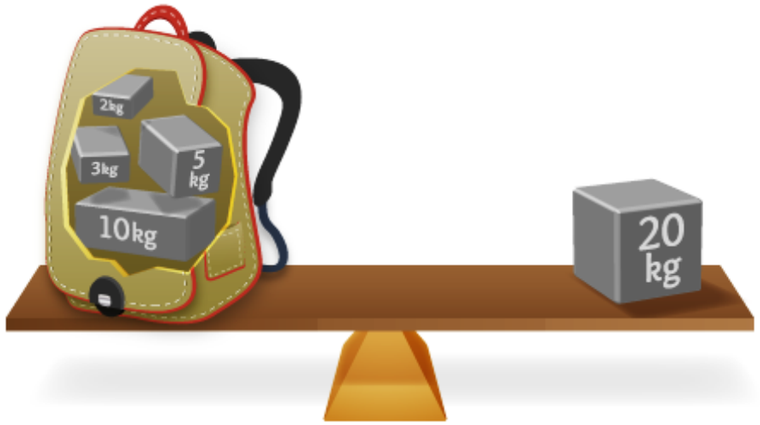
2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Задача рюкзака

Дано набір предметів різної маси. Чи можна покласти деякі із цих предметів у рюкзак так, щоб маса рюкзака дорівнювала певному значенню?

Задача: за вагою рюкзака визначити, які предмети поклали, а які ні

Наприклад, маси предметів 1, 5, 6, 11, 14 і 20. Можна спакувати рюкзак так, що його маса дорівнюватиме 22, використавши маси 5, 6 і 11. Неможливо спакувати рюкзак так, щоб його маса дорівнювала 24



2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Ідея шифрування повідомлення як розв'язання задачі рюкзака

Дано набір значень $M_1, M_2,\ldots, M_n$ і сума S, обчислити значення b_i, такі що $S = M_1 b_1 + M_2 b_2 + \ldots + M_n b_n$, $b_i \in \{0,1\}$

$M_1, M_2,\ldots, M_n$ – рюкзак;
$b_1, b_2,\ldots, b_n$ – відкритий текст;
S – шифротекст

Приклад 2.1:

Відкритий текст	111001	010110	000000	011000
Рюкзак	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14 20
Шифротекст	1+5+6+20=32	5+11+14=30	0=0	5+6=11

2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Задача рюкзака

Легка

Якщо перелік мас предметів являє собою суперзростаючу послідовність, то задачу рюкзака легко розв’язати

Складна

Якщо перелік мас предметів являє собою нормальну послідовність, то задачу рюкзака розв’язати важко

2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Суперзростаюча послідовність – це послідовність, у якій кожний елемент більший за суму усіх попередніх елементів

Нормальна послідовність – це послідовність, що містить довільні елементи

Наприклад, послідовність {1, 3, 6, 13, 27, 52} є суперзростаючою

Наприклад, послідовність {1, 3, 4, 9, 15, 25} не є суперзростаючою, тобто вона нормальна

2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Алгоритм розв'язання задачі суперзростаючого рюкзака

1. Повну вагу рюкзака порівнюємо з найбільшим числом послідовності

2. Якщо повна вага менша за це число, то його не кладемо у рюкзак

3. Якщо повна вага більша або дорівнює цьому числу, то воно кладеться у рюкзак. Зменшуємо масу рюкзака на це значення

4. Переходимо до наступного по величині числа послідовності

5. Будемо повторювати, поки процес не закінчиться. Якщо повна вага зменшиться до нуля, то розв’язок знайдений

2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Приклад 2.2:

Повна вага рюкзака – 70, послідовність мас {2, 3, 6, 13, 27, 52}

1. Найбільша маса – 52 < 70 ⇨ кладемо 52 у рюкзак.
2. Віднімаємо: 70-52=18.
3. Наступна маса – 27 > 18 ⇨ 27 у рюкзак не кладемо.
4. Вага 13 < 18 ⇨ кладемо 13 у рюкзак.
5. Віднімаємо: 18-13=5.
6. Наступна маса – 6 > 5 ⇨ 6 не кладемо у рюкзак.

Продовження цього процесу покаже, що й 2, і 3 кладемо у рюкзак, і повна вага зменшується до 0, що повідомляє про знайдений розв’язок.

Відкритий текст: 110101

2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Криптосистема Меркла-Хелмана

Закритий ключ – суперзростаюча послідовність

Відкритий ключ – нормальна послідовність

Генерування відкритого ключа із закритого

1. Генерується суперзростаюча послідовність

2. Обирається число *m* (модуль), більше за суму усіх чисел послідовності

3. Знаходиться *n* взаємно просте з *m*

4. Усі значення суперзростаючої послідовності множаться по модулю *m* на число *n*

2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Приклад 2.3:

Дано: закритий ключ – супер зростаюча послідовність {2, 3, 6, 13, 27, 52}, m = 105, n = 31

Нормальною послідовністю буде:
2·31 mod 105 = 62
3·31 mod 105 = 93
6·31 mod 105 = 81
13·31 mod 105 = 88
27·31 mod 105 = 102
52·31 mod 105 = 37

Відкритий ключ – {62, 93, 81, 88, 102, 37}

2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Шифрування у криптосистемі Меркла-Хелмана

1. Розбити повідомлення на блоки, рівні по довжині кількості елементів послідовності рюкзака.

2. Вважати, що у відкритому тексті одиниця вказує на присутність члена послідовності, а нуль – на його відсутність.

3. Обчислити повні маси рюкзака – по одному для кожного блоку повідомлення.

2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Приклад 2.4:

Дано: повідомлення в бінарному виді 011000110101101110,
відкритий ключ – послідовність {62, 93, 81, 88, 102, 37}

Шифруємо: повідомлення = 011000 110101 101110
011000 відповідає 93 + 81 = 174
110101 відповідає 62 + 93 + 88 + 37 = 280
101110 відповідає 62 + 81 + 88 + 102 = 333

Шифротекст: послідовність {174, 280, 333}

2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Дешифрування у криптосистемі Меркла-Хелмана

1. Спочатку визначають n^{-1}, таке що n (n^{-1}) ≡ 1 (mod m)

2. Кожне значення шифротексту множиться на n^{-1}mod m

3. Одержати значення відкритого тексту за допомогою закритого ключа – одиниця вказує на присутність члена послідовності, а нуль – на його відсутність

2. Алгоритм рюкзака (криптосистема Меркла-Хелмана)

Приклад 2.5:

Дано: шифротекст {174, 280, 333}, закритий ключ – {2, 3, 6, 13, 27, 52},
m =105, n = 31

Дешифруємо:

У нашому випадку n^{-1} дорівнює 61, тому значення шифротекста помножимо на 61 mod 105.

$174 \cdot 61 \bmod 105 = 9 = 3 + 6$, що відповідає 011000

$280 \cdot 61 \bmod 105 = 70 = 2 + 3 + 13 + 52$, що відповідає 110101

$333 \cdot 61 \bmod 105 = 48 = 2 + 6 + 13 + 27$, що відповідає 101110

Відкритий текст: 011000 110101 101110

3. Симетричні шифри vs асиметричні шифри

Характеристика	Симетричні шифри	Асиметричні шифри
Ключ	Один і той самий ключ використовується для шифрування та дешифрування	Один ключ (відкритий) використовується для шифрування, інший (закритий) – для дешифрування
Обмін ключами	Потрібен секретний канал для передачі ключа або інший надійний механізм обміну ключами	Відкритий ключ доступний всім, але його справжність має перевірятися центром сертифікації ключів
Математична складність	Відносно прості математичні операції	Складні математичні обчислення
Швидкість роботи	Висока	Низька
Криптографічна стійкість	Задовільна	Достатня
Вид захисту	Конфіденційність	Конфіденційність, цілісність, автентичність, невідмовність