# 5.2. Сервіси миттєвого обміну повідомленнями

**Exchange Instant Messaging Service** - технологія обміну повідомленнями та файлами між двома і більше абонентами через Інтернет або іншу мережу в режимі реального часу. Можуть передаватися текстові повідомлення, звукові сигнали, зображення, відео, а також проводитися такі дії, як спільне малювання або ігри. Багато з таких сервісів можуть застосовуватися для організації групових текстових чатів або відеоконференцій. Сьогодні, коли в одиницю часу приймається і обробляється велика кількість інформації, дана технологія є просто незамінною.

Система миттєвих повідомлень працює за деяким протоколом. Протоколи бувають серверні або безсерверні. Найпоширенішими є серверні протоколи, коли месенджери не працюють самостійно, а підключаються до центрального сервера мережі обміну повідомленнями.

У безсерверних протоколах (FChat, NASSI, UChat) повідомлення передаються безпосередньо від одного співрозмовника до іншого.

Сервіси Instant Messaging подібні до електронної пошти, але мають істотну відмінність - обмін інформацією (текстовими, графічними, відео та іншими файлами) відбувається в реальному часі. За допомогою спеціальних індикаторів надається можливість отримання додаткової інформації в режимі реального часу, наприклад, чи знаходиться співрозмовник на даний момент в мережі і чи він прочитав надіслане повідомлення.

У ранніх версіях програм передача повідомлення відбувалася прямо під час друкування, було видно всі набрані слова та їх виправлення. В такому режимі спілкування нагадувало телефонну розмову. В сучасних програмах повідомлення з'являються на моніторі співрозмовника вже після завершення редагування і надсилання повідомлення.

Технології Instant Messaging сьогодні прагнуть забезпечити високий рівень безпеки переданої інформації та захист від проникнення хакерів чи вірусів. Особливо це небезпечно для користувачів, які проводять комерційне листування, де певний обсяг конфіденційної інформації може бути доступний на серверах, які не перебувають під контролем самої компанії.

### Месенджер програма-клієнт для служби миттєвого обміну повідомленнями

Майже для кожного сервісу миттєвого обміну повідомленнями розроблено власну програму – месенджер. Більшість користувачів бачать лише клієнтську частину месенджера - це або програма на комп'ютері, або додаток на мобільному пристрої. Всі месенджери зав'язані на власні сервера - там відбувається зберігання інформації і обробка даних. Серверна частина забезпечує безпеку акаунтів, зберігає історію спілкувань та контакти.

Кожен з месенджерів працює за власним протоколу передачі даних і ці протоколи рідко бувають сумісними. Розробники кожного з месенджерів прагнуть до того, щоб користувачі ставили тільки їх застосування (можна увімкнути рекламу або запропонувати платну послугу). Тому, різні месенджери майже завжди несумісні між собою і для того, щоб спілкуватися людям доводиться встановлювати кілька додатків одночасно.

Особливості месенджерів:

* Миттєва передача повідомлень. Можливість передавати текст, картинки, відео, довільні файли.
* Можливість вести голосову і відео розмову без додаткової плати за зв'язок, оплачується лише Інтернет трафік.
* Відображення статусу співрозмовника (активний чи немає в мережі) і повідомлення (прочитане чи ні).
* Збереження історії листування.

## Компоненти системи

Кожна система миттєвого обміну повідомленнями повинна мати такі складові:

* Система ідентифікації (адресації) клієнтів.
* Система обліку стану клієнтів (хто підключений, а хто ні)
* Система доставки повідомлень (зазвичай, передає повідомлення через комп'ютерну мережу, але може наприклад безпосередньо до іншого користувача на тому самому комп'ютері)

### Система ідентифікації (адресації) клієнтів

У безсерверних протоколів виникають проблеми ідентифікації співрозмовника. Для точної ідентифікації клієнта вони можуть використовувати лише фізичну мережну адресу (IP). Це створює складність, оскільки на одному комп'ютері можуть знаходитися декілька користувачів. Для вирішення цієї проблеми створено серверні протоколи.

У серверних протоколах виділяється сервер, який проводить облік користувачів. На сервері потрібно зареєструватися використовуючи ідентифікатор та пароль (необов'язково).

Ідентифікатори користувачів — це зазвичай номер (ICQ) або спеціальне ім'я користувача (логін). В деяких протоколах (наприклад, XMPP Jabber) логін подібно до електронних адрес містить домен і має вигляд ім'я\_користувача@домен

### Система обліку стану користувачів

Більшість месенжерів дозволяє користувачам бачити, чи під’єднані до мережі їхні співрозмовники в цей момент, так званий статус.

Існує три основних статуси, що відображають присутність/відсутність користувача у мережі:

1. В мережі / Онлайн (Online) — користувач під'єднаний до мережі і готовий до спілкування.
2. Не в мережі / Офлайн (Offline) — користувач поза мережею.
3. Невидимий (Invisible) — користувач знаходиться в мережі, але цей спеціальний статус не дозволяє бачити його всім іншим (або лише деяким) користувачам. Натомість вони бачать статус користувача як: «не в мережі».

Більшість протоколів дозволяє використовувати багато статусів і вони можуть містити заданий користувачем текст (наприклад «Зайнятий, пишу дипломну» або «Вийшов в магазин») і додаткове зображення-іконку. Зазвичай, використовуються такі статуси:

* Відійшов (Away). Традиційно вмикається коли користувач деякий час не користується комп'ютером. Може бути встановлений самим користувачем коли він відходить від комп'ютера або вмикатися автоматично самою програмою-клієнтом завдяки реєстрації часу бездіяльності користувача.
* Недоступний (N/A — Non-Available). Традиційно вмикається коли користувач довгий час не користується комп'ютером. Може вмикатися автоматично самою програмою-клієнтом завдяки реєстрації часу бездіяльності користувача.
* Зайнятий (Busy).
* Не турбувати (DND — Do Not Disturb).
* Готовий побалакати (Free for Chat).
* Вдома (At home).
* На роботі (At work).
* Їм (Eating).
* Злий (Evil).

### Список контактів

Користувач може створювати власний список контактів. Контакти можуть бути згруповані у групи з назвою. Більшість протоколів дозволяють зберігати список контактів на сервері, що створює певні зручності:

* Користувач може отримати його, знаходячись на іншому комп'ютері.
* Користувач може задавати власні правила для контактів. Наприклад, список заблокованих (заборонених) контактів, від яких він не бажає отримувати повідомлення («чорний список»). Або список контактів, для яких його статус завжди видимий.
* Користувач може зберігати власні примітки для контактів

### Система збереження повідомлень

Повідомлення можуть бути збережені у журналі (історії) повідомлень. Цей журнал може бути переглянутий. Деякі протоколи (GTalk/XMPP) дозволяють, так само як і контакти, зберігати журнал на сервері.

### Інформація про користувачів

Майже всі поширені протоколи (окрім IRC) дозволяють користувачам задавати власну інформацію про себе у спеціальних анкетах. Деякі протоколи (XMPP) використовують для цього стандарт так званої візитної картки VCard. Зазвичай, анкети містять такі поля як:

* Нік (нікнейм, псевдонім).
* Справжнє ім'я.
* Фотографія користувача або зображення (аватар).
* Адреса.
* Дата народження та вік.
* Інтереси.
* Про себе.
* Контактна інформація (електронна пошта, номери телефонів та інше).

## Популярні месенжери

### Skype

Безкоштовне програмне забезпечення з закритим кодом, що забезпечує текстовий, голосовий та відеозв'язок через Інтернет між комп'ютерами (IP-телефонія), а також надає платні послуги для дзвінків на мобільні і стаціонарні телефони. Спочатку Skype було представлено у вигляді програми для персонального комп'ютера, що орієнтована на голосовий та відео зв'язок між користувачами. З поширенням мобільних пристроїв для цього месенджера створено мобільний додаток.

Більшої популярності Skype мав, коли не було гідного конкурента, але з часом Viber, WhatsApp, Telegram виявилися більш зручними. Після придбання Skype компанією Microsoft месенджер став працювати значно повільніше, що пов'язано з поступовою інтеграцією сервісу в Windows. Також, невдалі зміни інтерфейсу та правила використання зменшили ряди прихильників даного месенджеру.

### Viber

Програма, яка дозволяє здійснювати безкоштовні дзвінки через мережу Wi-Fi або мобільні мережі, надсилати текстові повідомлення, зображення, відео та аудіо повідомлення, документи і файли. Додаток працює як на мобільних телефонах, так і на персональних комп'ютерах. Акаунти в Viber прив'язуються до номера мобільного телефону, що робить дуже простим пошук людей через стандартну записну книжку.

### logo-whatsappWhatsApp

Популярна безкоштовна система миттєвого обміну текстовими повідомленнями для мобільних та інших платформ з підтримкою голосового і відеозв'язку. Дозволяє пересилати текстові повідомлення, зображення, відео та аудіо через Інтернет. Даний месенджер подібний за функціоналом до Viber. Акаунт в WhatsApp відповідає номеру телефону, список контактів береться безпосередньо із записника телефону.

### Facebook Messenger

Всі функції Facebook Messenger спрямовані на те, щоб надати можливість користувачу спілкуватися з друзями на Facebook, не заходячи при цьому в саму соціальну мережу. Рішення Facebook звільнити Messenger від соціальної мережі та перетворити його в автономний додаток, було неоднозначно сприйнято користувачами. По-перше, це створило необхідність встановлювати ще один додаток на свій пристрій. По-друге, користувачі повинні були зробити «додатковий крок», якщо вони хотіли поспілкуватися один з одним.

З часом Facebook Messenger перетворився в унікальний інструмент, корисний не лише для контакту з друзями. Зайти в свій акаунт на Facebook Messenger можна через діючий акаунт на Facebook та використовуючи мобільний номер телефону. Месенджер повністю синхронізує всі дані з Facebook, зберігаються історія повідомлень та налаштування акаунту.

Широкий функціонал і простота використання Facebook Messenger роблять його одним з найбільш зручних на ринку мобільних платформ, що виправдовує його популярність.

**Telegram**

Багатоплатформний месенджер для смартфонів, що позиціонується як захищений засіб спілкування та дозволяє обмінюватися повідомленнями і медіафайлами в багатьох форматах.

Використовується пропрієтарна серверна частина c закритим кодом, що працює на потужностях кількох компаній США і Німеччини. Месенджер Telegram має версію для різних типів пристроїв, встановлюється і на комп'ютер і на смартфон з будь-якою операційною системою.

Месенджер більше орієнтований на комерційну аудиторію, там, де доводиться вести групові обговорення і не можна допустити витоку інформації. Це забезпечують захищені протоколи і налаштування, зокрема автоматичне видалення повідомлень через заданий період часу. В Telegram є можливість створювати канали та здійснювати в них односторонню трансляцію повідомлень – пише лише автор, інші читають - це аналог підписки на оновлення, типу поштових розсилок (спам не надсилається, оскільки підписка робиться особисто).

На жаль, Telegram не підтримує аудіо та відео дзвінків, що робить його незручним для приватних бесід, коли хочеться чути і бачити співрозмовника.

#### Причини популярності Telegram

* **Політика приватності.** Завдяки новій технології шифрування, повідомлення захищені від перехоплення. Інформація зберігається в дата-центрах у вигляді окремо зашифрованих кластерів. Зберігання даних реалізовано на базі хмарних технологій.
* **Кросплатформність.** Розміщення інформації в хмарі дозволяє працювати з даними з будь-якого пристрою.
* **Швидкість роботи.** Надсилання повідомлень займає частки секунди, завдяки розміщенню дата-центрів в 5 регіонах.
* **Відкритість.** Основа програми - API MTProto, як і код самого програмного забезпечення, перебуває у вільному доступі.
* **Безоплатність.** Додаток Telegram - некомерційний продукт, і, як обіцяють автори, залишиться безкоштовним. Відсутність реклами.
* **Підтримка**. Розробники враховують побажання користувачів і проект постійно вдосконалюється та розвивається.
* **Безпека.** Автори пообіцяли 200 тисяч американських доларів тому, хто зможе витягнути і розкодувати інформацію. За роки існування програми досі це не вдалося нікому.

#### Особливості Telegram

* Пошук контактів для спілкування, використовуючи не номер телефону, а нікнейм користувача в Telegram.
* Одночасний захід в акаунт з 2-3 і більше пристроїв, з мобільних та декстоп-версій.
* Спілкування всередині секретного чату для 2-х осіб, коли повідомлення користувачів не зберігаються в хмарі, а передаються на гаджети і знищуються після прочитання. Самоліквідація повідомлення при встановленні відповідного таймера у відправника і одержувача.
* Організація групових чатів Telegram, що підтримують до 200 контактів з фільтрацією за критеріями всередині чату (є варіант суперчатів до 5 000 користувачів).
* Опція редагування повідомлень через певний час після передачі.
* Миттєве надсилання файлів величиною до 1,5 гігабайтів (архівів, таблиць Excel, файлів PDF, аудіо в MP3, відео).
* Зберігання інформації в зашифрованому вигляді - 99% безпеки. Навіть отримавши доступ до серверів в дата-центрі, зловмисник не зламає листування користувачів, оскільки ключі до розшифрування зберігаються в іншому дата-центрі.
* Використання ботів для покращення роботи акаунту Telegram, збору статистики, зв'язки з громадськістю, рекламних та інших цілей.

# Наскрізне шифрування

Наскрізне шифрування (end-to-end encryption, кінцеве шифрування) - це коли дзвінки, повідомлення, відео, аудіо, зображення, документи та інші дані доступні лише для співрозмовників та захищені від попадання в треті руки. Ключі шифрування є також тільки у них. За допомогою цих ключів можна розблокувати і прочитати повідомлення.

У кожного чату є свій код безпеки, який використовується для підтвердження наскрізного шифрування повідомлень. Його можна знайти в розділі «Дані контакту» у вкладці «Шифрування» у вигляді QR-коду або 60-значного номера.

Код безпеки - це видима версія спеціального ключа. Повна версія ключа тримається в секреті. Крім того, кожне відправлене повідомлення має індивідуальний замок і ключ. Все це відбувається автоматично - користувачеві не треба нічого налаштовувати.

Популярність наскрізного шифрування зросла в 2013 році, після того як Едвард Сноуден опублікував документи, що доводять, що уряд США відстежує кожен дзвінок і відправлене повідомлення. Після цього технологічні гіганти, такі як Apple і Facebook, вирішили убезпечити приватне життя своїх користувачів і ввели наскрізне шифрування.

Наскрізне шифрування (E2EE) шифрує повідомлення протягом усього його шляху між двома кінцевими точками. Воно залишається зашифрованим під час транспортування через проміжні сервери, і ані постачальник послуг ані провайдер ані будь-яка третя сторона не може отримати до нього доступ.

Без E2EE повідомлення шифрується, як тільки доходить до центрального сервера, який розшифровує його. Таким чином, об'єкт, керуючий цими серверами (наприклад, провайдер послуг інтернет), може бачити повідомлення користувача. Однак, якщо використовувати VPN, цей тип з'єднання набагато безпечніше, оскільки VPN служба шифрує трафік і змінює IP користувача. Тоді можна безпечно і конфіденційно пройти через всі проміжні точки.

### Основні способи шифрування даних.

**Симетричні криптосистеми** передбачають, що для шифрування і дешифрування застосовується один і той же криптографічний ключ. Головний недолік полягає в тому, що ключ повинен бути розділений між сторонами. Якщо не буде створено безпечний тунель, перехоплювач зможе тягнути ключ і розшифрувати повідомлення (рис.1).

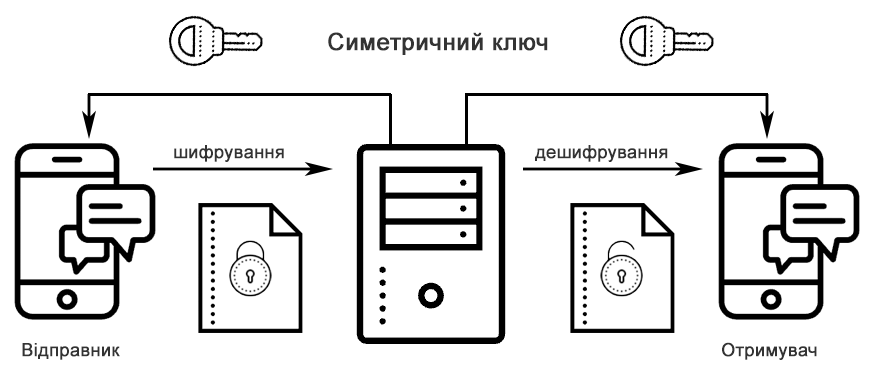


Рис.1. Симетричне шифрування

Щоб забезпечити стійкість криптосистеми від зламу, до даних застосовуються алгоритми, необхідні для захисту. Самого ключа недостатньо, необхідно перемішати дані таким чином, щоб забезпечити надійність. Однак за наявності досить великих продуктивних потужностей ключ можна підібрати. Щоб вирішити цю проблему, фахівці безпеки збільшують такі параметри, як довжина ключа, складність і число раундів перетворення.

**Асиметричне шифрування.** Для захисту даних використовуються два ключі - відкритий і закритий. Відкритий потрібен для шифрування даних, але для розшифрування він абсолютно даремний. З цієї причини він доступний всім, хто хоче спілкуватися з хранителем закритого ключа. Тільки за допомогою закритого ключа можна розшифрувати дані (рис.2).

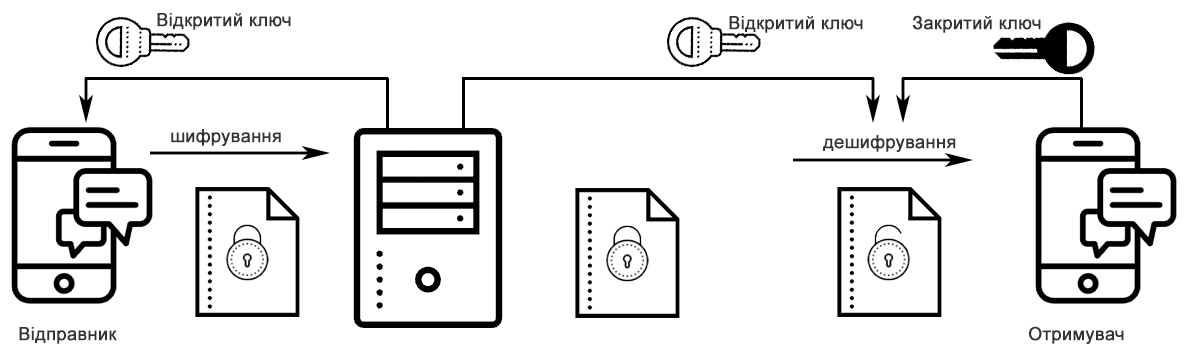


Рис.2. Асиметричне шифрування

Наскрізне шифрування може комбінувати ці два методи. У випадку з месенджерами ключі локалізовані каналом зв'язку і відомі тільки для клієнтів, що спілкуються між собою. Захищений канал дозволяє виключити атаки методом «людини посередині». Таким чином дані, які він перехопить, будуть марні.

Ключовою характеристикою месенджерів, що використовують наскрізне шифрування, є приватність і анонімність. Під приватними даними розуміють, що жодні дані не доступні для третіх осіб. У найпопулярніших месенджерів є певні напрацювання в цьому напрямку. Наприклад, Telegram має функцію самознищення акаунту у разі відсутності активності користувача. Це рішення надає «право на забуття». Те, що опубліковано кілька років тому, може стати «незаконним контентом» з можливістю притягнення до відповідальності.

Анонімність месенджерів виражається в тому, що зв'язок встановлюється через сервера компанії, і IP-адреса віддаленого користувача є прихованою, а клієнт в свою чергу не знає ІР-адресу сервера.

Технології зв'язку, реалізовані в клієнтах, можуть мати й недоліки. Наприклад, в WhatsApp при інтернет-дзвінках існує можливість отримати реальну IP-адресу користувача навіть без встановленого сеансу зв'язку.

Недолік всіх месенджерів - авторизація за номером мобільного телефону. Спецслужби багатьох країн мають доступ до мобільних провайдерів зв'язку і можуть надсилати СМС з номера користувача без будь-яких повідомлень і користувач про це навіть не дізнається. Для захисту від цього в багатьох месенджерах передбачено функцію оповіщення про активність користувача за допомогою іншого пристрою. Крім того, список використовуваних клієнтів доступний в налаштуваннях.

## Проблеми

### Атака «людина посередині»

Наскрізне шифрування передбачає, що контроль за листуванням здійснюється безпосередньо користувачами. Одним з варіантів обходу наскрізного шифрування для зловмисника є захоплення під свій контроль каналу зв'язку між кінцевими точками, після цього він може спробувати видати себе за одержувача повідомлення, щоб, наприклад, підмінити відкритий ключ. Щоб не дати себе виявити, зловмисник після дешифрування повідомлення може зашифрувати його ключем, який він або вона поділяє з фактичним одержувачем, або його або її відкритим ключем у випадку асиметричних систем, і знову відправити повідомлення. Атаки такого типу прийнято називати атаками «людина посередині».

Для запобігання MITM-атак більшість криптографічних протоколів використовують автентифікацію. Для цього можуть використовуватися, наприклад, центри сертифікації. Альтернативним методом є створення відбитків відкритого ключа на основі загальнодоступних відкритих ключів користувачів або загальних секретних ключів. Перш ніж почати розмову сторони порівнюють свої відбитки відкритих ключів з використанням зовнішнього каналу зв'язку, який гарантує цілісність та автентичність зв'язку, при цьому він не обов'язково повинен бути секретним. Якщо відбитки пальців збігаються, значить атака «людина посередині» не була проведена.

### Безпека кінцевих точок

Іншим способом обходу наскрізного шифрування є атака безпосередньо на кінцеві точки доступу. Кожний пристрій користувача може бути зламано, з метою вкрасти криптографічний ключ (для створення атаки «людина посередині») або просто прочитати дешифровані повідомлення користувачів. Для уникнення такого роду спроб злому, необхідно забезпечити відповідний захист пристроїв за допомогою програмних або інших методів.

Основними спробами підвищити безпеку кінцевих точок були виведення ключових операцій генерації, зберігання і криптографії на смарт-карту. Але, оскільки введення і виведення відкритого тексту видно в системі, то ці підходи не здатні захистити від клавіатурних шпигунів і шкідливого програмного забезпечення, яке може відстежувати розмови в режимі реального часу. Більше надійний підхід полягає у фізичній ізоляції пристрою.

### Backdoor

Backdoor (Back door – задні двері)- шкідлива програма, а іноді навмисно залишена лазівка в коді легальної програми, яка надає доступ до пристрою для несанкціонованих дій. Бекдор в точності відповідає своїй назві: приховано впускає зловмисника в систему, наділяючи правами адміністратора.

Компанії можуть також (самостійно чи з примусу) впроваджувати у своє програмне забезпечення бекдори, які допомагають порушити узгодження ключа або обійти шифрування.

Альянс «П'ять очей» (Five Eyes), куди входять розвідслужби США, Великобританії, Австралії, Канади та Нової Зеландії, вимагають від технологічних компаній впроваджувати бекдори в зашифровані додатки, щоб можна було надати правоохоронним органам доступ, необхідний для припинення кіберзлочинності. За словами вищих посадових осіб, зростання кількості додатків з наскрізним шифруванням, таких як Signal, Telegram, FaceBook Messenger і WhatsApp, «створюють серйозні проблеми для громадської безпеки».

«Хоча шифрування має життєво важливе значення, а головним пріоритетом повинна бути конфіденційність і кібербезпека, це не повинно здійснюватися за рахунок повного виключення можливості правоохоронних органів і самої технологічної індустрії протистояти небезпечному незаконному контенту і діяльності в інтернеті», - пояснили чиновники.

Прихильники захисту конфіденційності стверджують, що впровадження бекдору, за допомогою яких правоохоронні органи зможуть отримати доступ до повідомлень користувача, може поставити під загрозу дисидентів і посилити вплив деяких диктаторських урядів.

Згідно інформації, розкритої Едвардом Сноуденом в 2013 році, Skype містив бекдор, який дозволяв Microsoft передавати в АНБ повідомлення користувачів, незважаючи на те, що офіційно ці повідомлення піддавалися наскрізному шифруванню.

## Контрольні питання

1. Які послуги надають сервіси миттєвих повідомлень?
2. Перелічити компоненти системи миттєвих повідомлень.
3. Яку інформацію показує система обліку стану користувачів?
4. Яка інформація про користувача міститься в месенжері?
5. Провести порівняльний аналіз популярних месенжерів.
6. Пояснити причини популярності Telegram.
7. Назвати причини, з яких причин користувачі встановлюють Facebook Messenger? Які переваги від нього має користувач Facebook?
8. Порівняйте якісні характеристики WhatsApp та Viber: зручність інтерфейсу, якість зв’язку, наявність реклами, додавання контактів, групові чати.
9. Для чого використовують наскрізне шифрування в месенжерах?
10. Назвати особливості симетричного шифрування?
11. Назвати особливості асиметричного шифрування?
12. Які існують варіанти обходу наскрізного шифрування?

## Література

1. Шифрування в месенджерах <https://xakep.ru/2018/06/14/useless-encryption/>
2. Криптографія для початківців <https://bitnovosti.com/2020/07/16/kriptografiya-dlya-absolyutnyh-novichkov/>
3. Основи алгоритмів шифрування <https://hacker-basement.ru/2019/08/23/kryptografia-dlay-hakerov-algorytmy-shifrovaniy/>
4. Що таке наскрізне шифрування? <https://bezopasnik.info/что-такое-сквозное-шифрование-типы-ши/>
5. Функції Viber <https://www.viber.com/ru/features/>
6. Корисні функції в WhatsApp <https://androidinsider.ru/polezno-znat/38-funktsij-v-whatsapp-o-kotoryh-vy-ne-znali-chast-1.html>
7. Приховані можливості Facebook Messenger <https://daily.afisha.ru/brain/5394-11-funkciy-facebook-messenger-pro-kotorye-vy-mogli-ne-znat/>
8. Переваги Telegram перед аналогічними продуктами <https://nastroyvse.ru/programs/review/vozmozhnosti-telegram-na-fone-analogichnyx-produktov.html>
9. Як влаштовано шифрування в месенджерах <https://thecode.media/dh/>
10. Безпека переписки в месенджерах <https://safe-surf.ru/users-of/article/666973/>
11. Офіційний сайт Skype - <https://www.skype.com/uk/>
12. Офіційний сайт Viber - <https://www.viber.com/ru/>
13. Офіційний сайт WhatsApp - <https://www.whatsapp.com/?lang=uk>
14. Офіційний сайт Telegram - <https://telegram.org/>
15. Офіційний сайт Facebook Messenger - <https://www.messenger.com>