

УДК 004.4

В. Б. Гурський; Т. Р. Кульчицький

(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВПЛИВ ШИФРУВАННЯ НА ПРОДУКТИВНІСТЬ ВЕБСАЙТІВ: ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ АЛГОРИТМІВ

UDC 004.4

V. B. Hurskiy; T. R. Kulchytskyi

THE IMPACT OF ENCRYPTION ON WEBSITE PERFORMANCE: A COMPARATIVE ANALYSIS OF MODERN ALGORITHMS

1. Значення шифрування для сучасних вебсайтів

- **Забезпечення конфіденційності та безпеки даних**

Шифрування є основою для захисту особистої інформації користувачів, особливо при передаванні даних через Інтернет (наприклад, HTTPS). Воно мінімізує ризик перехоплення та злому даних.

- **Обов'язковість у сучасних стандартах**

Усі сучасні вебсайти мають використовувати HTTPS, що базується на TLS (Transport Layer Security), для відповідності вимогам пошукових систем і підвищення довіри користувачів.

- **Вплив на SEO**

Пошукові системи (наприклад, Google) надають перевагу сайтам із шифруванням, підвищуючи їх у рейтингу.

2. Типи алгоритмів шифрування, що застосовуються у вебсайтах

- **RSA (Rivest–Shamir–Adleman)**

- **Особливості:** Широко використовуваний алгоритм асиметричного шифрування для встановлення з'єднань.
- **Недоліки:** Високе навантаження на процесор через складність обчислень, особливо з великими ключами (2048/4096 біт).
- **Переваги:** Високий рівень захисту.

- **ECDSA (Elliptic Curve Digital Signature Algorithm)**

- **Особливості:** Менші ключі зберігають такий самий рівень безпеки, як і RSA, але працюють швидше.
- **Вплив на продуктивність:** Менше використання обчислювальних ресурсів.

- **AES (Advanced Encryption Standard)**

- **Особливості:** Симетричний алгоритм, що забезпечує швидке шифрування. Зазвичай використовується у HTTPS після встановлення з'єднання.
- **Переваги:** Енергоефективний, підходить для великих обсягів даних.

- **ChaCha20 + Poly1305**

- **Особливості:** Більш ефективний для пристроїв із низькою продуктивністю, таких як мобільні телефони.
- **Переваги:** Швидкий і сучасний, особливо для нестандартних умов з'єднання.

3. Як шифрування впливає на продуктивність вебсайтів

- **Затримки при встановленні з'єднання**
Алгоритми асиметричного шифрування (RSA, ECDSA) впливають на швидкість першого встановлення TLS-з'єднання. Чим складніший алгоритм і більший ключ, тим більше часу потрібно.
- **Ресурси сервера**
Використання складних алгоритмів шифрування збільшує навантаження на сервери. Це може бути критичним для сайтів із великим трафіком.
- **Затримки під час передачі даних**
Симетричні алгоритми, такі як AES, швидше шифрують дані під час передачі, але все одно додають невеликі накладні витрати.
- **Оптимізація з'єднань**
Використання HTTP/2 і TLS 1.3 значно зменшують накладні витрати шифрування, зменшуючи кількість «рукописок» і оптимізуючи процес передачі.

4. Порівняльний аналіз продуктивності алгоритмів

- **RSA vs ECDSA**
RSA забезпечує високу безпеку, але його повільніша продуктивність робить його менш ефективним порівняно з ECDSA, особливо в мобільних мережах.
- **AES vs ChaCha20**
AES працює ефективніше на сучасних процесорах із підтримкою апаратного шифрування (AES-NI), тоді як ChaCha20 кращий для мобільних пристроїв і старіших процесорів.
- **TLS 1.2 vs TLS 1.3**
TLS 1.3 швидший за TLS 1.2 завдяки меншій кількості рукописок і оптимізованому алгоритму шифрування.

5. Шляхи оптимізації використання шифрування

- **Вибір правильного алгоритму для аудиторії сайту**
Для мобільних користувачів варто використовувати ChaCha20, тоді як для стаціонарних серверів оптимальним є AES із апаратною підтримкою.
- **Використання TLS 1.3**
Це новий стандарт, який дозволяє значно зменшити затримки й підвищити продуктивність.
- **Кешування та стиснення даних**
Використання стиснення (наприклад, Brotli) зменшує обсяг переданих даних, а кешування TLS-з'єднань (Session Resumption) скорочує час повторного підключення.

6. Висновки

Шифрування є критично важливим компонентом сучасних вебсайтів, але воно має певний вплив на продуктивність. Правильний вибір алгоритму та технологій шифрування дозволяє забезпечити баланс між безпекою і швидкістю роботи вебсайту. У майбутньому, із розвитком обчислювальних технологій, продуктивність шифрування буде ще кращою.