Nama : Rifko Satrio Rahmadani
Email : ikosatriorahmadani@gmail.com
Pekerjaan : Mahasiswa
Nama Instansi/Sekolah : Politeknik Negeri Bandung

Challenge Penggunaan Cryptography

1. Bagaimana cara membuktikan bahwa website yang anda buka Adalah Gmail asli?

   Jawab:

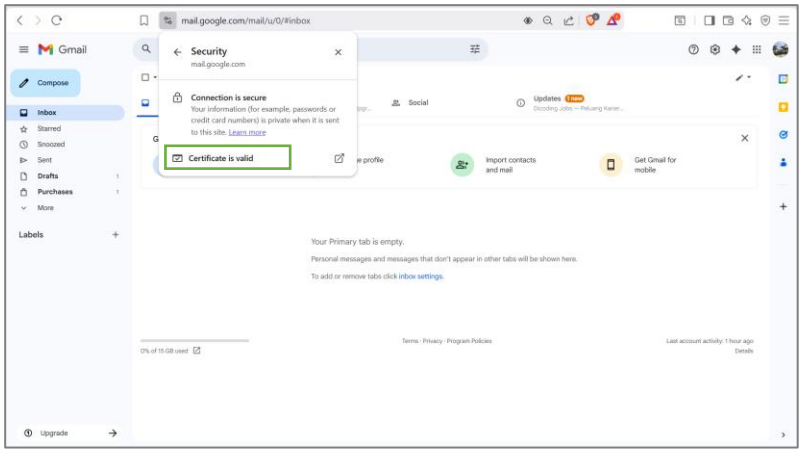
   Untuk memastikan kalau website yang saya buka benar-benar Gmail asli, saya cek bagian sertifikat HTTPS-nya di browser. Biasanya saya klik ikon gembok di sebelah kiri alamat URL, lalu melihat informasi sertifikatnya. Dari situ akan terlihat siapa Certificate Authority (CA) yang menandatangani, kepada siapa sertifikat itu diterbitkan, dan apakah statusnya valid.

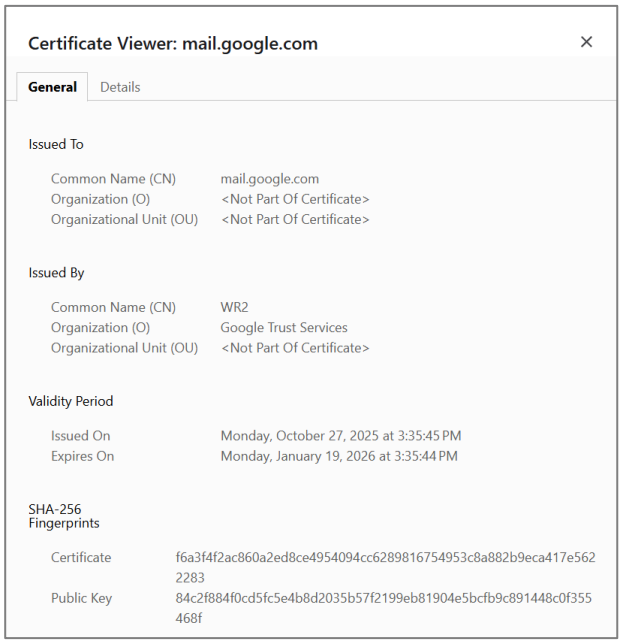
   Kalau sertifikatnya diterbitkan untuk domain google.com oleh CA yang terpercaya dan statusnya valid, berarti website tersebut memang Gmail asli dan bukan situs palsu.

2. Screen Shot Digital Certificate yang digunakan?

   Jawab:

   Saya membuka https://gmail.com lalu mengeklik ikon gembok di samping alamat URL. Setelah itu, saya memilih menu Connection is secure untuk melihat informasi sertifikat, kemudian mengambil screenshot seperti di bawah ini.





3. Apakah nama dari CA yang digunakan gmail?

   Jawab:

   Berdasarkan informasi pada sertifikat, Gmail menggunakan CA dengan nama "WR2" yang dikeluarkan oleh Google Trust Services.

4. Apakah CA tersebut termasuk kedalam CA Public atau Private? Sebutkan alasannya!

   Jawab:

   CA yang digunakan adalah Google Trust Services, dan itu termasuk Public CA. Alasannya, karena sertifikat dari Google Trust Services dipercaya secara otomatis oleh browser umum (Chrome, Edge, Firefox) tanpa harus menambahkannya secara manual. Jadi sertifikatnya memang dibuat untuk publik dan dipakai oleh layanan internet besar seperti Gmail.

5. Dikeluarkan untuk siapa Digital Certificate tersebut?

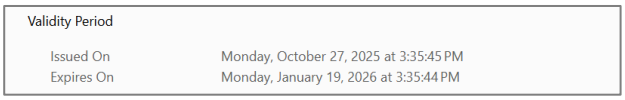
   Jawab:

   Sertifikat tersebut dikeluarkan untuk domain mail.google.com, yang terlihat pada bagian Issued To → Common Name (CN).

6. Kapan Digital Certificate tersebut kadaluarsa?

   Jawab:

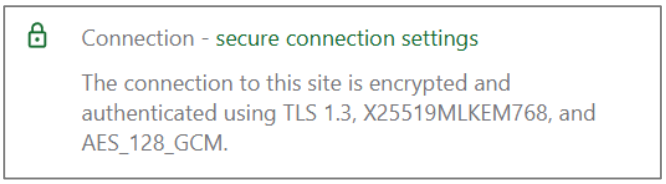
   Expires On → Monday, January 19, 2026 at 3:35:44 PM



7. Algoritma apakah yang digunakan untuk mengenkripsi komunikasi dengan gmail?

   Jawab:

   Gmail memakai TLS 1.3 dengan X25519 sebagai key exchange dan AES-128-GCM sebagai algoritma enkripsinya.



8. Algoritma hash apa yang digunakan untuk fingerprint Digital Certificate tersebut?

   Jawab:

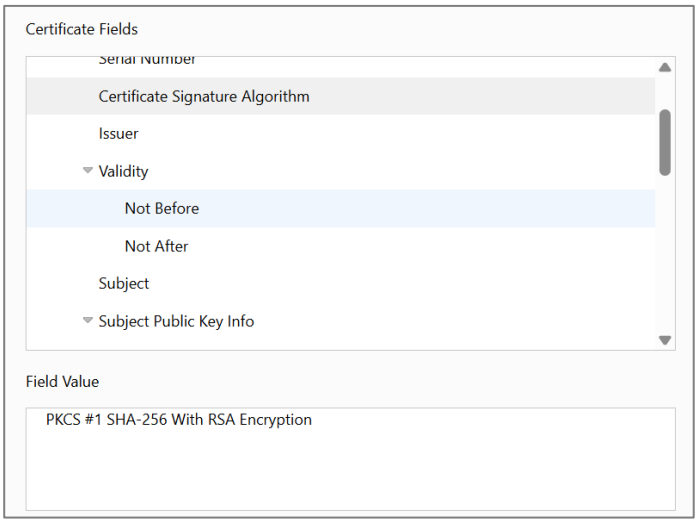
   Fingerprint di certificate Gmail menggunakan algoritma hash SHA-256.

9. Algoritma apakah yang digunakan untuk signatur Digital Certificate tersebut?

   Jawab:

   Digital certificate Gmail ditandatangani menggunakan algoritma SHA-256 with RSA encryption.

   PKCS #1 SHA-256 With RSA Encryption



10. Kunci yang digunakan untuk melakukan enkripsi komunikasi anda dengan gmail Adalah?

    Jawab:

    Gmail menggunakan AES-128 GCM sebagai kunci enkripsi utama saat komunikasi berlangsung. Kunci ini dihasilkan setelah proses handshake TLS 1.3. Jadi semua data yang aku kirim/terima dari Gmail diamankan oleh kunci simetris AES-128.