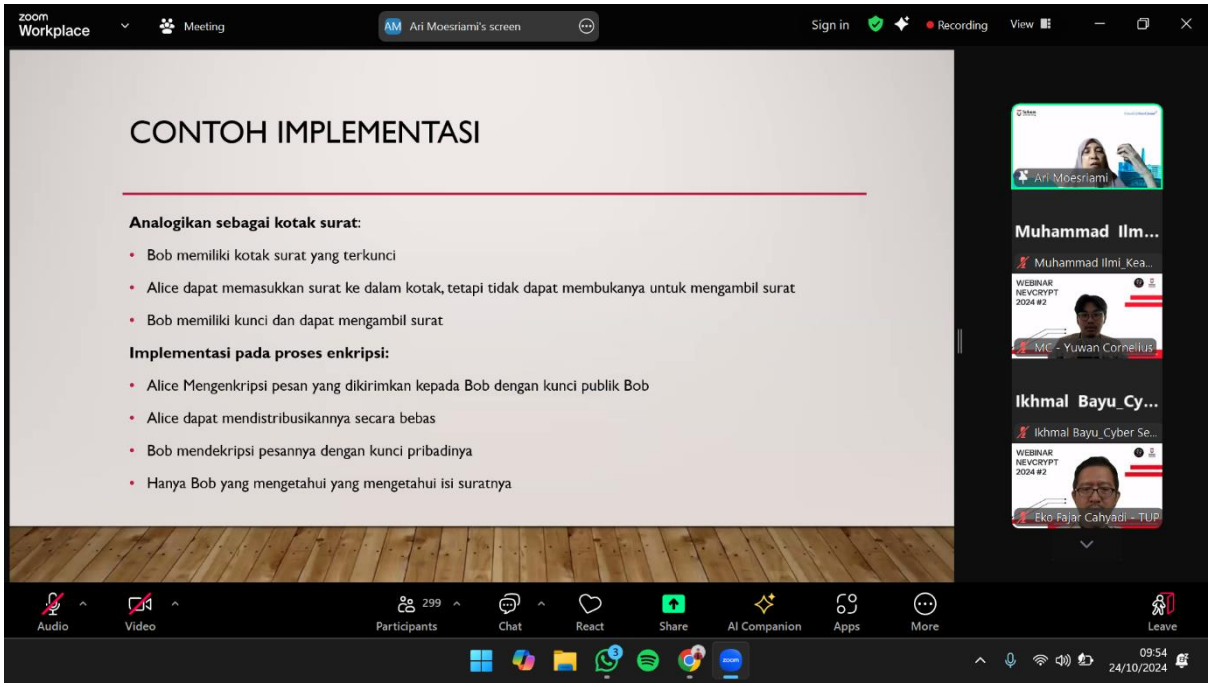
Nama : Muhammad Ilmi

NIM : 21102070

Kelas : Keamanan Siber (IF-09-02)

Webinar NevCrypt - Asymmetric Cryptography



RESUME ASYMMETRIC CRYPTOGRAPHY

Definisi Kriptografi Asimetrik

Menggunakan pasangan kunci—kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Pesan yang dienkripsi dengan kunci publik hanya dapat didekripsi oleh kunci privat yang terkait.

Konsep Dasar

Melibatkan enkripsi menggunakan kunci publik dan dekripsi menggunakan kunci privat, memungkinkan pertukaran informasi yang aman tanpa perlu berbagi kunci dekripsi.

Contoh Implementasi

Diilustrasikan melalui analogi kotak surat, di mana kunci publik adalah akses untuk memasukkan pesan, sementara kunci privat diperlukan untuk membacanya.

Persyaratan Kriptografi Asimetrik

Tiga Syarat Utama:

1. Enkripsi dan dekripsi harus mudah jika kunci yang sesuai digunakan.
2. Tidak ada cara mudah untuk mengekstrak pesan dari kunci publik.
3. Keamanan terhadap serangan berbasis teks biasa, sehingga penyerang tidak bisa mengembalikan teks asli hanya dengan memiliki pesan terenkripsi.

Algoritma Kriptografi Asimetrik Awal

RSA dan El Gamal adalah contoh awal dari algoritma kunci publik, dengan proses enkripsi dan dekripsi yang mengandalkan operasi matematika kompleks.

RSA:

- Dibuat dengan memilih dua bilangan prima besar (p, q), lalu mengalikan untuk membentuk nilai n.
- Kunci publik terdiri dari (n, e) dan kunci privat terdiri dari (n, d).
- Proses Enkripsi : $c = m^e \ mod \ n$
- Proses Dekripsi : $m = c^d \ mod \ n$

El Gamal:

- Berdasarkan fungsi satu arah, menggunakan perhitungan mod p (bilangan prima).
- Proses enkripsi dan dekripsi dilakukan dalam dua langkah terpisah yang memerlukan bilangan acak untuk menghasilkan ciphertext yang unik setiap kali.

Kelebihan dan Kekurangan Metode

Metode asimetrik umumnya lebih aman dibandingkan simetrik, tetapi prosesnya lebih lambat dan memerlukan ukuran kunci yang lebih besar. Rentan terhadap serangan "man-in-the-middle" dan tidak efisien terhadap serangan kuantum.

Post-Quantum Cryptography

- **Kebutuhan Baru:**
  Kriptografi asimetrik klasik seperti RSA tidak mampu bertahan terhadap serangan komputer kuantum.
- **Teknologi Baru:**
  1. McEliece Cryptosystem
     Tahan terhadap serangan kuantum, menggunakan matriks paritas untuk mengaburkan pesan.
  2. Learning With Errors (LWE)
     Menyembunyikan pesan dalam serangkaian persamaan linier yang dilengkapi dengan gangguan acak.