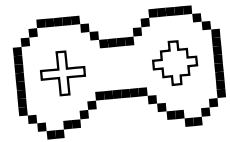
Praktikum Kriptografi

Pertemuan - 12A

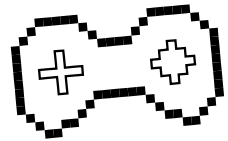
Topik: Kuis

Peraturan



1. Kuis dilaksanakan berupa 4 soal esai.
2. Pengerjaan bisa dilakukan secara tulis tangan atau melalui Ms Word.
3. Jelaskan secara rinci pengerjaan step-by-step untuk proses enkripsi dan dekripsi, penghitungan bisa dibantu dengan Ms Excel atau kalkulator (bukan kalkulator dcode.fr yak).
4. Hasil pengerjaan dibuat menjadi file **NPM_Kuis2.pdf** dan dikumpulkan ke kantong classroom di akhir sesi kuis.
5. Silakan kerjakan dengan jujur dan teliti.

Soal 1



Lakukan proses enkripsi dan dekripsi dari nama depan kalian menggunakan RSA dengan diketahui parameternya :

- **p = 59**
- **q = 89**

Waktu : 20 menit

Soal 2

Gunakan kriptografi S-DES untuk mengenkripsi sebuah plaintext dengan ketentuan berikut:

Pt = ASCII Digit Pertama NPM

Master Key = ASCII Digit Akhir NPM + 10

P_{10} = 3 5 2 7 4 10 1 9 8 6

P_8 = 6 3 7 4 8 5 10 9

P_4 = 2 4 3 1

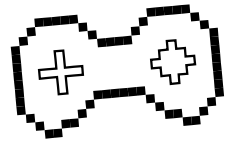
Substitution Box:

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

	0	1	2	3
0	0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	3	2	1	0	3

Waktu : 30 menit

Soal 3



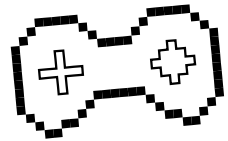
Diketahui persamaan kurva eliptik $y^2 \equiv x^3 + 7x + 10 \ (mod\ 23)$

Lakukan enkripsi dengan diketahui parameter:

- **Plaintext: (8,3)**
- α **= (3,9)**
- **q = 3**
- **r = 2**

Waktu : 25 menit

Soal 4



Diketahui sebuah persamaan kurva eliptik sebagai berikut

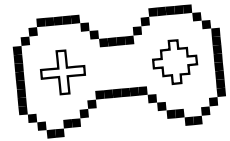
$$y^2 \equiv x^3 + 3x + 30 \ (mod\ 23)$$

Lakukan enkripsi menggunakan kriptografi **Menezes-Vanstone ECC** dengan ketentuan sebagai berikut

- **Pt = (4,7)**
- α **= (3,9)**
- **q = 4**
- **r = 3**

Waktu : 15 menit

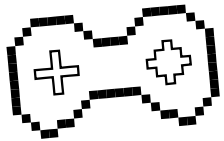
Project UAS



1. Buat kelompok dengan anggota **maks. 3 orang**
2. Silahkan isi kelompok pada link Kelompok Kriptografi
3. **Pilih topik** yang tersedia pada link tersebut
4. Lalu, dari topik yang kalian pilih, silakan **buat sebuah aplikasi kriptografi sederhana** untuk algoritma tersebut (boleh web, android, atau apapun), **penggunaan GUI akan mendapat nilai plus**
5. Waktu pengerjaan 2 minggu, dengan ketentuan:

   - Minggu depan → Presentasi Progress 1 + Konsultasi Algoritma

   - 2 Minggu depan → Presentasi Project Final



Thank You!!

Kalau misalkan ada pertanyaan,
yaudah tanya aja

Praktikum Kriptografi 2022

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**

Please keep this slide for attribution