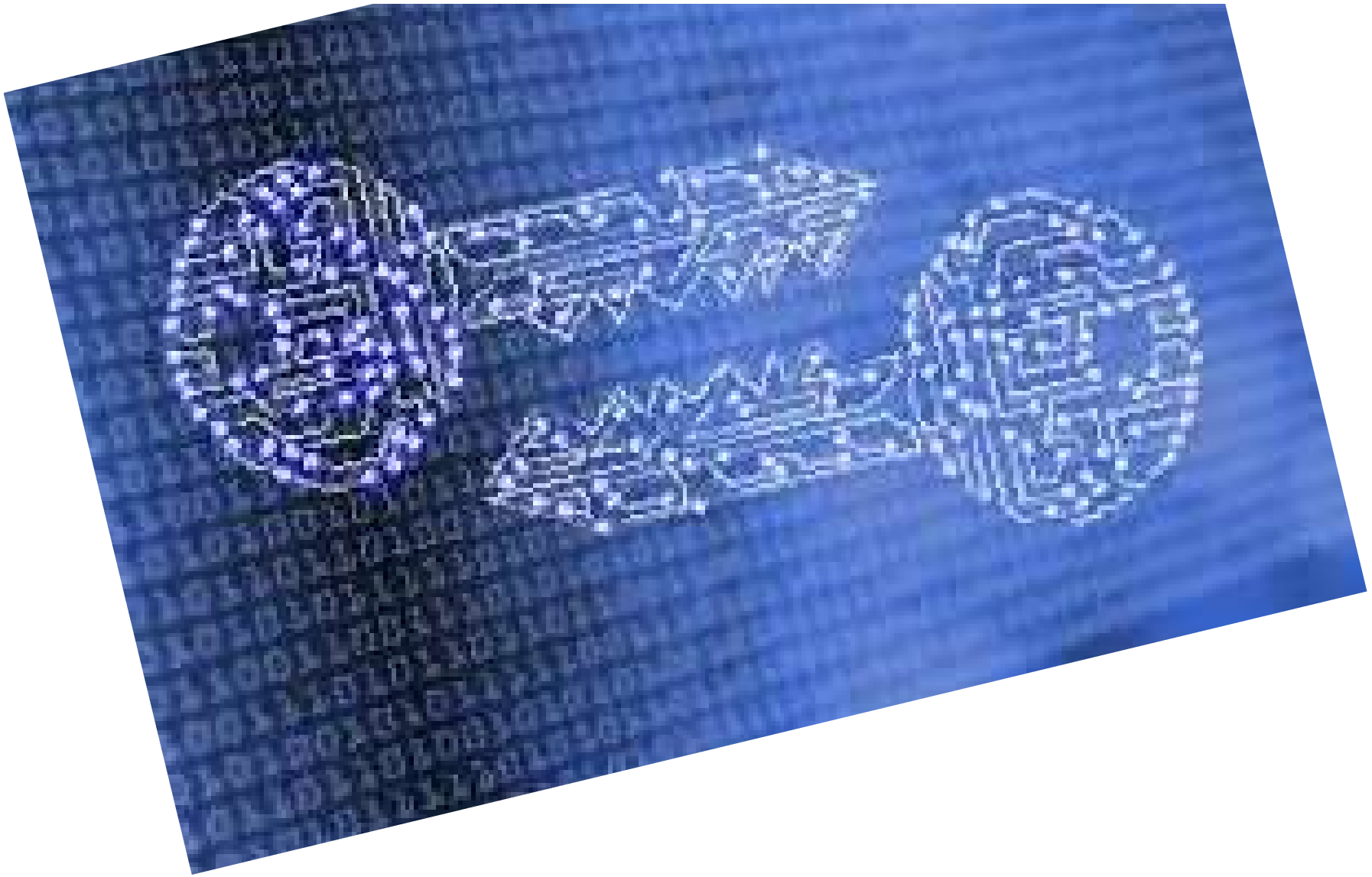
Kriptografi

03. Cipher Polialfabetik & Analisis Kelemahan

Kodrat Mahatma

Universitas Teknologi Digital



“Mengapa panjang kunci penting dalam keamanan kriptografi?”

Cipher Polialfabetik & Analisis Kelemahan

- Memahami Prinsip Vigenère Cipher dan Teknik Analisisnya
- Progress Tugas dan Q and A

Tujuan Pembelajaran

1. Menjelaskan prinsip dasar Cipher Polialfabetik.
2. Menerapkan Vigenère Cipher untuk enkripsi dan dekripsi.
3. Melakukan analisis frekuensi dan serangan Kasiski.
4. Mengidentifikasi kelemahan dan mitigasinya.

Konsep Dasar

- Cipher Polialfabetik menggunakan beberapa alfabet untuk mengenkripsi teks.
- Contoh paling terkenal: Vigenère Cipher.

Rumus Matematis Vigenère Cipher

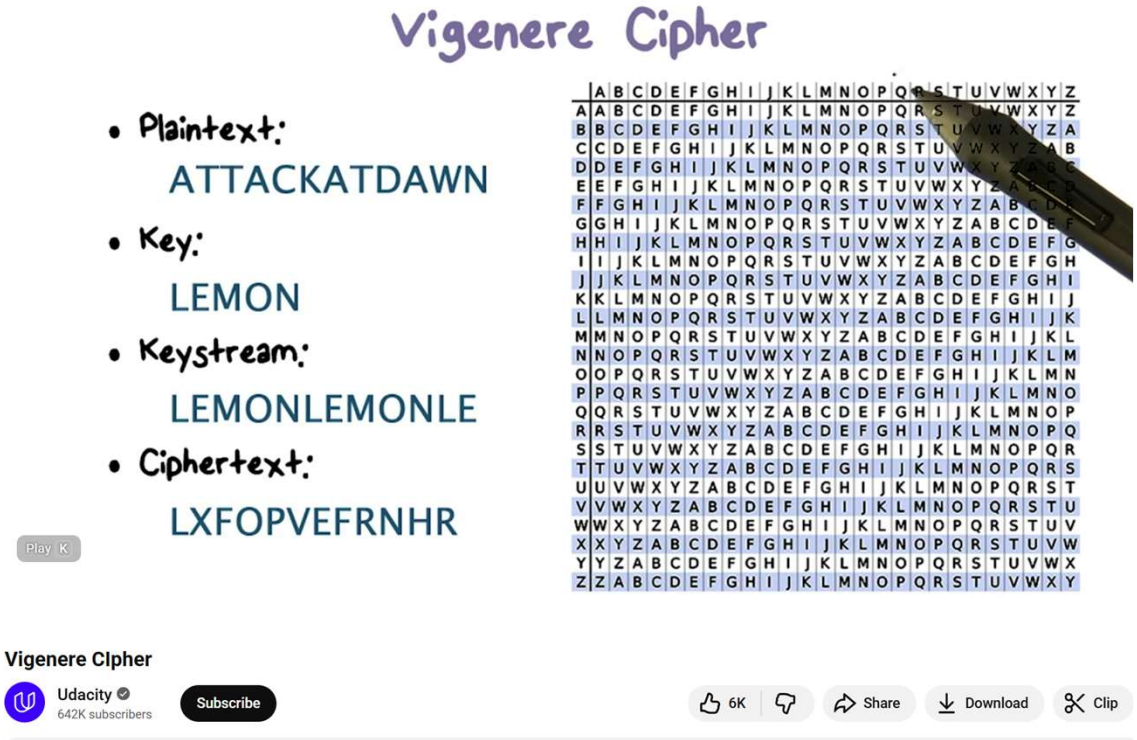
- Enkripsi: Ci = (Pi + Ki) mod 26
- Dekripsi: Pi = (Ci - Ki) mod 26
- Keterangan: P = plaintext, C = ciphertext, K = kunci (A=0, B=1, …)

Contoh Enkripsi Vigenère

- Plaintext: CRYPTOGRAPHY
- Key: LEMON
- Ciphertext: NFFXZTTBDZNL

Vigenère Cipher – Konsep

- Menggunakan kata kunci untuk menentukan pergeseran setiap huruf.
- Contoh: Kunci = LEMON
- Plaintext = ATTACKATDAWN
- Ciphertext = LXFOPVEFRNHR



https://youtu.be/SkJcmCaHqSo?si=A3JfwsoEQJJVhD4Z

Tabel Vigenère (Vigenère Square)

- Tabel 26×26 huruf alfabet bergeser.
- Baris = huruf kunci,
- Kolom = huruf plaintext,
- Hasil = huruf cipher.

Implementasi Python – Enkripsi

```
def vigenere_encrypt(plain, key):
    res = ''
    for i in range(len(plain)):
        res += chr(((ord(plain[i]) - 65 + ord(key[i % len(key)]) - 65) % 26) + 65)
    return res

print(vigenere_encrypt('CRYPTOGRAPHY','LEMON'))
```

Implementasi Python – Dekripsi

```
def vigenere_decrypt(cipher, key):
    res = ''
    for i in range(len(cipher)):
        res += chr(((ord(cipher[i]) - ord(key[i % len(key)])) % 26) + 65)
    return res

print(vigenere_decrypt('NFFXZTTBDZNL','LEMON'))
print(vigenere_decrypt('LXFOPVEFRNHR','LEMON'))
```

Analisis Kelemahan Cipher Polialfabetik

1. Pola kunci pendek menghasilkan pola berulang.
2. Dapat diretas dengan analisis frekuensi periodik.
3. Panjang kunci dapat diidentifikasi dengan metode Kasiski atau Friedman.

Metode Kasiski Examination

Langkah:

1. Cari pola berulang pada ciphertext.
2. Hitung jarak antar kemunculan pola.
3. Faktor jarak memberi estimasi panjang kunci.

Metode Index of Coincidence (Friedman Test)

- IC = Σ [n_i (n_i - 1)] / [N (N - 1)]
- Nilai IC mendekati 0.066 → teks Inggris; mendekati 0.038 → acak.
- Gunakan perbedaan ini untuk mendeteksi panjang kunci.

Implementasi Python – Analisis Frekuensi

```
from collections import Counter
text='NFFXZTTBDZNL'
count=Counter(text)
for k,v in count.items():
 print(k,v/len(text))
```

Kelemahan & Solusi

- Kelemahan: pola berulang dan analisis frekuensi.
- Solusi: gunakan kunci panjang dan **one-time pad** untuk keamanan maksimal.

Praktikum – Analisis Kasiski

Langkah:

1. Gunakan CrypTool untuk mengenkripsi teks dengan kunci 3 huruf.
2. Lakukan analisis jarak antar-pola.
3. Uji hasil dengan memecahkan ciphertext.

No	Judul Video	Link	Catatan
1	Vigenere Encryption using CrypTool	https://www.youtube.com/watch?v=Py03rXc2m2s (YouTube)	Demonstrasi enkripsi/dekripsi Vigenère menggunakan CrypTool
2	Short Introduction to CrypTool 2	https://www.youtube.com/watch?v=dELT2-Vgsr8 (YouTube)	Memperkenalkan antarmuka dan fungsi CrypTool, berguna sebelum praktikum
3	CT2 – Cryptography for Everybody (CrypTool2 YouTube Channel)	https://www.youtube.com/c/CrypTool2/about (YouTube)	Channel resmi dengan berbagai video klasik termasuk Vigenère/Kasiski

Praktikum – Implementasi Python

1. Implementasikan enkripsi dan dekripsi Vigenère.
2. Tambahkan fungsi analisis frekuensi sederhana.
3. Visualisasikan hasil frekuensi dengan matplotlib.

Studi Kasus - Dekripsi

- Ciphertext: ‘LXFOPVEFRNHR’ dengan key = LEMON.
- Hasil dekripsi: ATTACKATDAWN.
- Analisis: menunjukkan pentingnya sinkronisasi antara kunci dan plaintext.

Perbandingan dengan Cipher Lain

Cipher	Tipe	Kelebihan	Kelemahan
Caesar	Monoalfabetik	Sangat mudah dipahami dan diimplementasikan	Sangat mudah diretas dengan brute-force atau analisis frekuensi
Vigenère	Polialfabetik	Lebih kuat dari Caesar, sulit dianalisis dengan frekuensi tunggal	Rentan jika panjang kunci pendek atau pola kunci berulang
One-Time Pad	Polialfabetik sempurna	Aman secara teoritis, tidak dapat diretas jika kunci acak dan tidak digunakan ulang	Tidak praktis karena kunci harus sepanjang pesan
Playfair Cipher	Poligrafik	Lebih sulit dipecahkan daripada substitusi tunggal, bekerja per pasangan huruf	Masih dapat diretas dengan analisis frekuensi pasangan
Hill Cipher	Poligrafik berbasis matriks	Menggunakan aljabar linear, kuat untuk pesan pendek	Rentan terhadap analisis jika matriks kunci diketahui

One-Time Pad (OTP)

One-Time Pad (OTP) adalah salah satu algoritma **kriptografi polialfabetik sempurna**, yang secara teoretis **tidak dapat diretas** — asalkan digunakan dengan benar.

🧩 Konsep Dasar

- Menggunakan **kunci acak (random key)** dengan **panjang yang sama** seperti pesan asli.
- Setiap huruf (atau bit) dari pesan dikombinasikan dengan kunci **sekali saja**, biasanya dengan operasi **XOR** (pada bit) atau **modular addition** (pada huruf).
- Setelah digunakan, kunci **harus dibuang dan tidak boleh digunakan ulang.**

🔐 Sifat Keamanan

✅ **Sempurna (Perfect Secrecy)** — sebagaimana dibuktikan oleh Claude Shannon (1949):

- Tanpa mengetahui kunci, ciphertext tidak memberikan *informasi statistik* apa pun tentang plaintext.
- Probabilitas menebak pesan benar-benar acak.

Tantangan	Penjelasan
Distribusi kunci	Kunci harus dikirim aman, sama panjang dengan pesan.
Penggunaan ulang kuncia	Jika digunakan ulang → dapat diretas (analisis XOR dua pesan).
Penyimpanan	Sulit dikelola untuk pesan panjang.
Tidak efisien	Tidak cocok untuk sistem komunikasi modern.

One-Time Pad (OTP)

🔢 Rumus Matematis

Untuk plaintext dan key yang direpresentasikan sebagai angka (A=0, B=1, ..., Z=25):

$$C_i = (P_i + K_i) \mod 26$$

$$P_i = (C_i - K_i) \mod 26$$

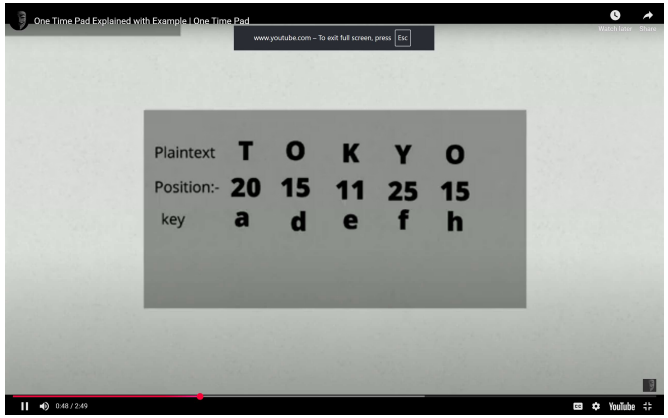
Keterangan:

- P_i = huruf ke-i dari plaintext
- K_i = huruf ke-i dari key
- C_i = huruf ke-i dari ciphertext

🚀 Aplikasi Nyata

Walau jarang dipakai luas, OTP masih digunakan dalam:

- **Sistem komunikasi diplomatik atau militer** yang membutuhkan keamanan mutlak.
- **Satelit dan komunikasi intelijen**, di mana kunci bisa didistribusikan secara fisik sebelumnya.



https://youtu.be/7Z6EewSy9p0

Aplikasi Modern

- Polialfabetik menjadi dasar enkripsi stream cipher modern.
- Contoh: RC4 (meskipun sudah deprecated) dan konsep kunci dinamis pada TLS awal.

Penugasan

1. Implementasikan Vigenère Cipher dan analisis frekuensinya.
2. Tulis laporan dengan hasil analisis ciphertext.
3. Gunakan CrypTool untuk validasi hasil.

Referensi & Bacaan

- Paar & Pelzl – Understanding Cryptography (Bab 1)
- Singh, The Code Book (1999)
- CrypTool Documentation – Vigenère Analysis
- Python Cryptography Cookbook

Sumber Belajar

No	Judul Video	Durasi	Deskripsi Ringkas	Link
1	**Index of Coincidence**	2:58	Penjelasan cepat tentang konsep Index of Coincidence untuk mendeteksi pola dalam ciphertext.	https://www.youtube.com/watch?v=kty-dCB4AAk
2	**The Index of Coincidence and Cryptanalysis of Shift Cipher**	2:47	Menunjukkan cara menghitung IC untuk memecahkan cipher klasik dengan pendekatan statistik.	https://www.youtube.com/watch?v=ZTFxzMScczw
3	**How To Write In Vigenère Cipher**	3:21	Tutorial singkat membuat dan membaca pesan dengan Vigenère Cipher secara manual.	https://www.youtube.com/watch?v=UuREH8tJjv4
4	**Polyalphabetic Part 1 – Vigenère Encryption and Kasiski**	~6:00	Pembahasan dasar cipher polialfabetik dan metode Kasiski examination untuk menemukan panjang kunci.	https://www.youtube.com/watch?v=LsewLHTAmsA
5	**Cryptanalysis: Breaking a Vigenère ciphertext with Kasiski's test**	4:11	Menunjukkan cara kerja Kasiski examination untuk menemukan panjang kunci.	https://youtu.be/Pl6AcJOEFvE?si=psIX6azT_Eq6NIVo

Sumber Belajar

No	Judul Video	Durasi	Deskripsi Ringkas	Link
1	**Tutorial Enkripsi Vigenere Cipher Sederhana**	2:50	Panduan praktis mengenkripsi teks menggunakan kunci sederhana di Python.	https://www.youtube.com/watch?v=dDH7B3TudrM
2	**ENKRIPSI VIGENERE CIPHER – Penjelasan dan Perhitungan**	2:43	Menjelaskan konsep dasar dan langkah enkripsi serta dekripsi.	https://www.youtube.com/watch?v=rRuMEHYYj5k
3	**KRIPTOGRAFI – Metode Vigenere Cipher**	3:10	Penjelasan ringkas tentang cara kerja cipher polialfabetik dan kelemahannya.	https://www.youtube.com/watch?v=hURVv2dxBeE
4	**Analisis Frekuensi & Kasiski dalam Kriptografi**	6:25	Demonstrasi analisis ciphertext dengan metode Kasiski menggunakan contoh teks nyata.	https://youtu.be/5QcnXdX2HMU?si=K2MfIHy9FJ8rt-U6

Penutup & Refleksi

“Keamanan cipher tidak bergantung pada algoritmanya, tetapi pada rahasia kuncinya.”

Selamat belajar !

‘Cryptography is the mathematics of trust.’