INSTITUT TEKNOLOGI DEL

MATERI PRAKTIKUM

KEAMANAN PERANGKAT LUNAK

SEMESTER GASAL TAHUN AJAR 2024/2025

Session Date	:	16 Oktober 2024
Semester	:	VI
Courses	:	Software Security / Keamanan Perangkat Lunak
Week/Session	:	02/03
Key Topics	:	Classical Encryption Techniques
Activity	:	• Mahasiswa melakukan review dengan menjawab soal yang diberikan sesuai dengan pemahaman teori dan konsep yang sudah diterima di sesi teori. • Mahasiswa dapat memecahkan studi kasus yang diberikan; • Mahasiswa dapat mengimplementasikan salah satu algoritma yang dipelajari.
Duration	:	170 menit
Delivery	:	Laporan Tugas di *file* nim_w02_ClassicalEncrytpionTechnicques.docx
Deadline of delivery	:	30 Oktober 2024, 17.00 WIB
Place of delivery	:	e-Course
Goal	:	Mahasiswa mampu memahami dan mampu menulis program untuk Teknik enkripsi klasik.

PENUGASAN:

Sebelum bekerja, setiap mahasiswa harus membaca instruksi di bawah ini.
Sangat disarankan bagi anda untuk:

1. Membaca soal-soal yang diberikan secara.
2. Mencari sumber-sumber lain seperti buku, artikel, bahkan video untuk memperkaya wawasan dan meningkatkan pemahaman anda.
3. Jika anda merasa ada hal yang belum dipahami, silakan untuk berkonsultasi pada TA.
4. Dengan demikian diharapkan anda mampu mengikuti materi kuliah dan praktikum sebaik mungkin.

Selamat Belajar & Good Luck!

Review Questions

1. What are the essential ingredients of a symmetric cipher?
2. What are the two basic functions used in encryption algorithms?
3. How many keys are required for two people to communicate via a cipher?
4. What is the difference between a block cipher and a stream cipher?
5. What are the two general approaches to attacking a cipher?
6. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
7. What is the difference between an unconditionally secure cipher and a computation-ally secure cipher?
8. Briefly define the Caesar cipher.
9. Briefly define the monoalphabetic cipher.
10. Briefly define the Playfair cipher.
11. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher?
12. What are two problems with the one-time pad?
13. What is a transposition cipher?

Problems

1. A ciphertext has been generated with an affine cipher. The most frequent letter of the ciphertext is “B,” and the second most frequent letter of the ciphertext is “U.” Break this code.
2. In one of his cases, Sherlock Holmes was confronted with the followingmessage.

   534 C2 13 127 36 31 4 17 21 41
   DOUGLAS 109 293 5 37 BIRLSTONE
   26 BIRLSTONE 9 127 171

   Although Watson was puzzled, Holmes was able immediately to deduce the type of cipher. Can you?
3. When the PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code:

   KXJEY UREBE ZWEHE WRYTU HEYFS
   KREHE GOYFI WTTTU OLKSY CAJPO
   BOTEI ZONTX BYBNT GONEY CUZWR
   GDSON SXBOU YWRHE BAAHY USEDQ

   The key used was “royal new zealand navy”. Decrypt the message. Translate TT into tt.
4. Using the Vigenère cipher, encrypt the word “explanation” using the key leg.

5. Encrypt the message “meet me at the usual place at ten rather than eight oclock” using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations and the result.

Programming Problems

1. Write a program that can encrypt and decrypt using the general Caesar cipher, also known as an Additive cipher.(NIM GANJIL)
2. Create software that can encrypt and decrypt using a 2 * 2 Hill cipher. (NIM GENAP)