PESU Center for
Information Security,
Forensics and
Cyber Resilience

Welcome to

PES University

Ring Road Campus, Bengaluru

10 June 2020

PESU Center for
Information Security,
Forensics and
Cyber Resilience

APPLIED CRYPTOGRAPHY

Lecture 6

Classical ciphers cryptanalysis

Without key get the secret data

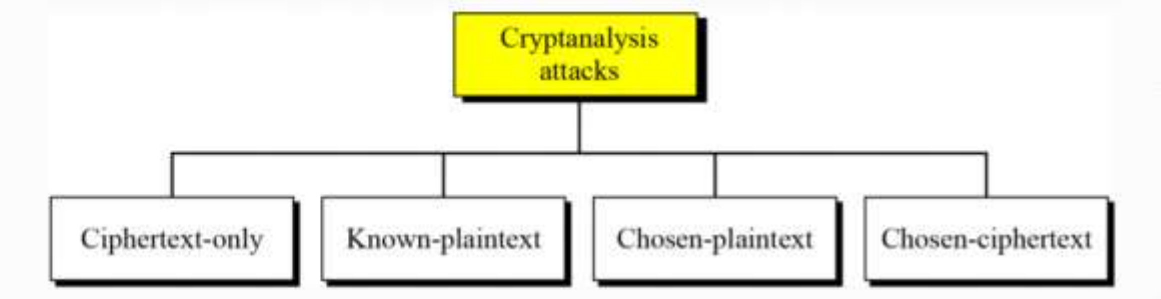
Cryptanalysis

- This video focus on cryptanalysis
- hacker wants to recover key or plaintext
- hacker is not bound by any rules
  - For example, hacker might attack the implementation, not the algorithm itself

Definition of Secure

- A cryptosystem is **secure** if the best know attack is to try all possible keys
- Cryptosystem is **insecure** if **any** shortcut attack is known
- By this definition, an insecure system might be harder to break than a secure system!

Cryptanalysis attack

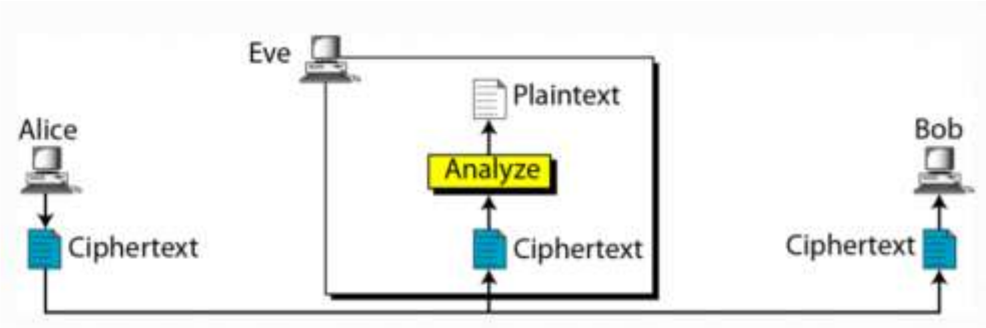


Cryptanalytic Attacks

- Ciphertext only
  - only know algorithm & ciphertext, is statistical, know or can identify plaintext
- Known plaintext
  - know/suspect plaintext & ciphertext
- Chosen plaintext
  - select plaintext and obtain ciphertext
- Chosen ciphertext
  - select ciphertext and obtain plaintext
- Chosen text
  - select plaintext or ciphertext to en/decrypt

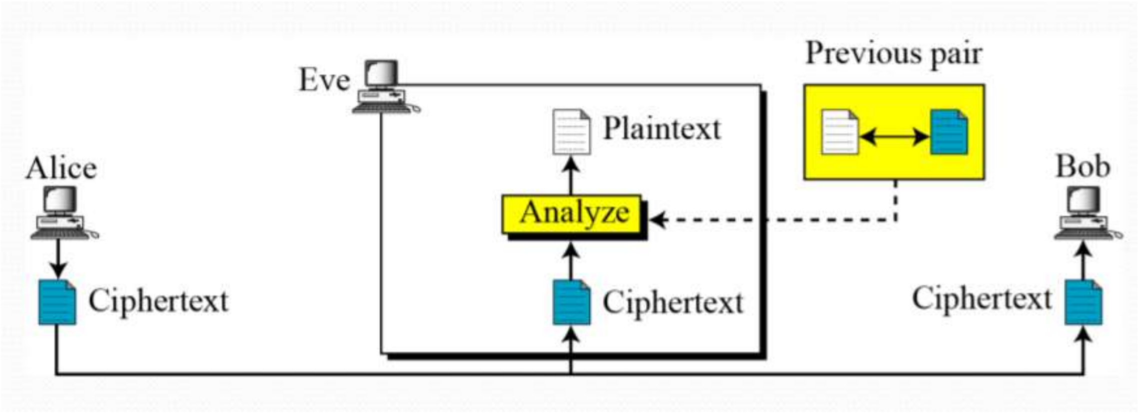
Ciphertext-Only Attack

- Ciphertext-only attack: only know algorithm & ciphertext, is statistical, know or can identify plaintext



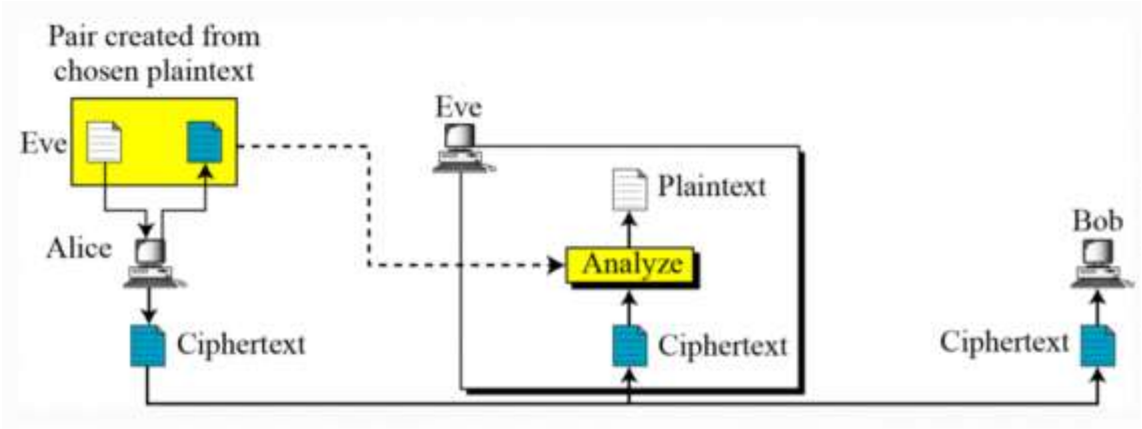
Known-Plaintext Attack

- know/suspect plaintext & ciphertext



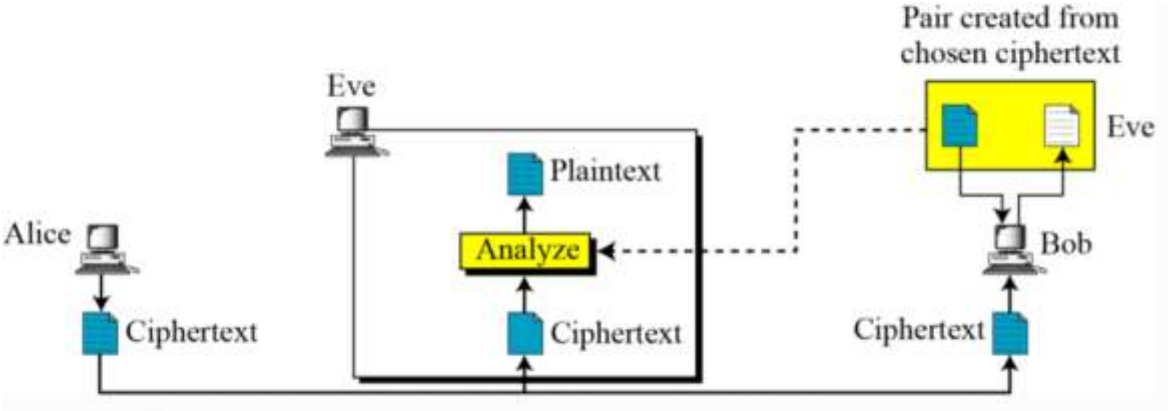
Chosen-Plaintext Attack

- select plaintext and obtain ciphertext



Chosen-Ciphertext Attack

- select ciphertext and obtain plaintext



Theoretical Cryptanalysis

- Think that a cipher has a 100 bit key
  - Then keyspace is of size 2^{100}
- Think there is a shortcut attack with “work” equal to testing about 2^{80} keys
- If hacker can test 2^{30} per second
  - Then she finds key in 36 million years
  - Better than 37 trillion, but not practical

Applied Cryptanalysis

- Classic (pen and paper) ciphers
  - Transposition, substitution, etc.
  - Same principles appear in later sections
- World War II ciphers
  - Enigma, Purple, Sigaba
- Stream ciphers
  - Shift registers, correlation attack, ORYX, RC4, PKZIP

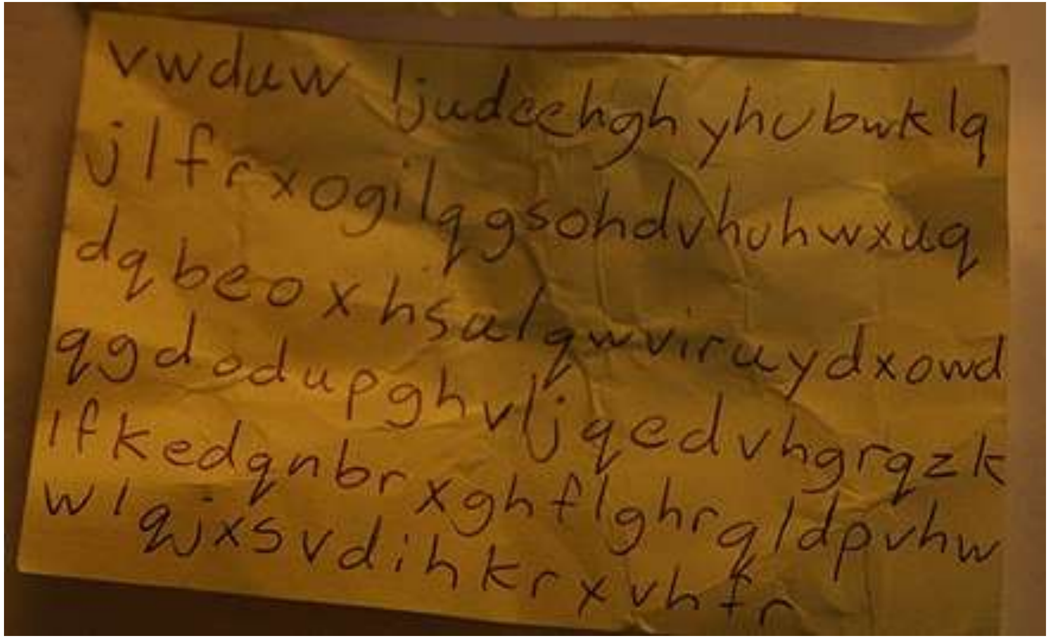
Why Study Cryptanalysis?

- Study of cryptanalysis gives insight into all aspects of crypto
- Gain insight into attacker’s mindset
  - “black hat” vs “white hat” mentality
- Cryptanalysis is more fun than cryptography
  - Cryptographers are boring
  - Cryptanalysts are cool
- But cryptanalysis is hard

Exhaustive Key Search

- try all possible keys and test each to see if it is correct
  - **Exhaustive key search**
- To prevent an exhaustive key search, a cryptosystem must have a large **keyspace**
  - Must be too many keys for Trudy to try them all in any reasonable amount of time

Cryptanalysis of Caesar cipher



vwduw ljudeehgh yhubwklq
jlfrxogilqgsohdvhohwxuq
dqbeoxhsdlqwvirudydxowd
qgdodupghvljqedvhgrqzk
lfkedqnbrxghflghrqldpvhw
wlqjxsvdihkrxvhfr

- https://www.khanacademy.org/computing/computer -science/cryptography/cryptochallenge/a/crypto-clue-1

Cryptanalysis of the Columnar Transposition Cipher

- The first step in attacking a columnar transposition cipher is to try all possible short keywords. If we check all keywords up to a length of 9 or so, we don't have to wait very long.
- For every keyword permutation we score the deciphered text, then choose the text with the highest score as our best candidate.
- The number of possible rearrangements of a

length N key is N! (N factorial). This number

grows very quickly as N gets larger.

Next Class

- ☞ Mandatory reading for the next class
  - ☞ https://brilliant.org/courses/probability/

S Rajashree

Computer Science and Engineering

PES University, Bengaluru