Introduction

Good Guys and Bad Guys

- Alice and Bob are the good guys


- Trudy is the bad guy

- Trudy is our generic "intruder"

Good Guys and Bad Guys

- Alice and Bob want to communicate securely
  - Typically, over a network
- Alice or Bob might also want to store their data securely
- Trudy wants to read Alice and Bob's secrets
- Or Trudy might have other devious plans…
  - Cause confusion, denial of service, etc.

CIA

- Confidentiality, Integrity and Availability
- **Confidentiality:** prevent unauthorized reading of information
- **Integrity:** prevent unauthorized writing of information
- **Availability:** data is available in a timely manner when needed
  - Availability is a "new" security concern
  - Due to denial of service (DoS) threats

Crypto

- **Cryptology** — The art and science of making and breaking "secret codes"
- **Cryptography** — making "secret codes"
- **Cryptanalysis** — breaking "secret codes"
- **Crypto** — all of the above (and more)

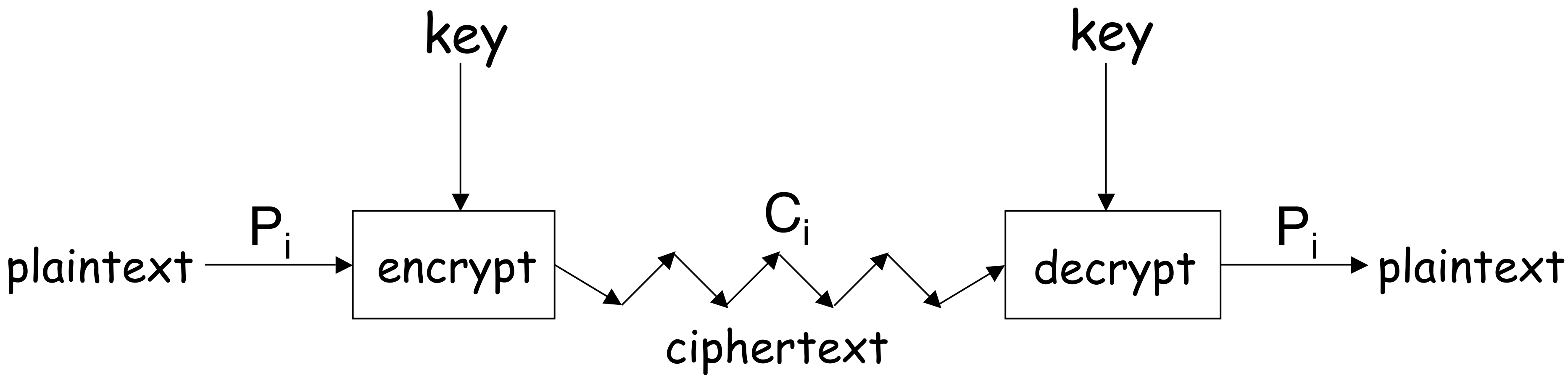
How to Speak Crypto

- A *cipher* or *cryptosystem* is used to *encrypt* the *plaintext*
- The result of encryption is *ciphertext*
- We *decrypt* ciphertext to recover plaintext
- A *key* is used to configure a cryptosystem
- A *symmetric key* cryptosystem uses the same key to encrypt as to decrypt
- A *public key* cryptosystem uses a *public key* to encrypt and a *private key* to decrypt
  - Private key can be used to sign and public key used to verify signature (more on this later…)

Crypto

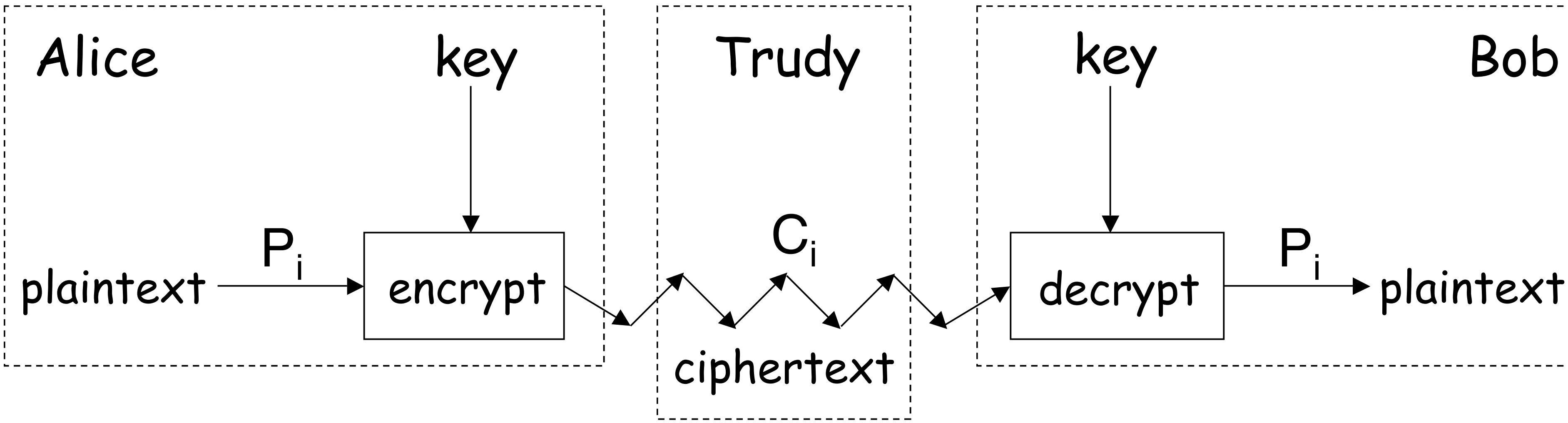
- Underlying assumption
  - The system is completely known to Trudy
  - Only the key is secret
- Also known as **Kerckhoffs Principle**
  - Crypto algorithms are not secret
- Why do we make this assumption?
  - Experience has shown that secret algorithms are often weak when exposed
  - Secret algorithms never remain secret
  - Better to find weaknesses beforehand

Crypto as a Black Box



- Note P_i is i^{th} "unit" of plaintext
- And C_i is corresponding ciphertext
- "Unit" may be bit, letter, block of bits, etc.

Who Knows What?



- Trudy knows the ciphertext
- Trudy knows the cipher and how it works
- Trudy might know a little more
- Trudy does **not** know the key

Taxonomy of Cryptography

- **Symmetric Key**
  - Same key for encryption as for decryption
  - Stream ciphers and block ciphers
- **Public Key**
  - Two keys, one for encryption (public), and one for decryption (private)
  - Digital signatures — nothing comparable in symmetric key crypto
- **Hash algorithms**

Cryptanalysis

- This course focused on cryptanalysis
- Trudy wants to recover key or plaintext
- Trudy is not bound by any rules
  - For example, Trudy might attack the implementation, not the algorithm itself
  - She might use "side channel" info, etc.

Exhaustive Key Search

- How can Trudy attack a cipher?
- She can simply 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

Beyond Exhaustive Search

- A large keyspace is necessary for security
- But a large keyspace is not sufficient
- Shortcut attacks might exist
- We'll see many examples of shortcut attacks
- In cryptography we can (almost) never prove that no shortcut attack exists
- This makes cryptography interesting…

Taxonomy of Cryptanalysis

- Ciphertext only — always an option
- Known plaintext — possible in many cases
- Chosen plaintext
  - "Lunchtime attack"
  - Protocols might encrypt chosen text
- Adaptively chosen plaintext
- Related key
- Forward search (public key crypto only)
- "Rubber hose", bribery, etc., etc., etc.

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!

Definition of Secure

- Why do we define **secure** this way?
- The size of the keyspace is the "advertised" level of security
- If an attack requires less work, then false advertising
- A cipher must be secure (by our definition) and have a "large" keyspace
  - Too big for an exhaustive key search

Theoretical Cryptanalysis

- Spse that a cipher has a 100 bit key
  - Then keyspace is of size 2^{100}
- On average, for exhaustive search Trudy tests $2^{100}/2 = 2^{99}$ keys
- Spse Trudy can test 2^{30} keys/second
  - Then she can find the key in about 37.4 trillion years

Theoretical Cryptanalysis

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

Applied Cryptanalysis

- In this class, we focus on attacks that produce plaintext
  - Not interested in attacks that just show a theoretical weakness in a cipher
- We call this **applied cryptanalysis**
- Why applied cryptanalysis?
  - Because it's a lot more fun…
  - And it's a good place to start

Applied Cryptanalysis: Overview

- 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

Applied Cryptanalysis: Overview

- Block ciphers
  - Hellman's TMTO, CMEA, Akelarre, FEAL
- Hash functions
  - Nostradamus attack, MD4, MD5
- Public key crypto
  - Knapsack, Diffie-Hellman, Arithmetica, RSA, Rabin, NTRU, ElGamal
  - Factoring, discrete log, timing, glitching

Why Study Cryptography?

- Information security is a big topic
  - Crypto, Access control, Protocols, Software
  - Real world info security problems abound
- Cryptography is the part of information security that works best
- Using crypto correctly is important
- The more we make other parts of security behave like crypto, the better

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