Ceng 520
Information Security and Cryptography

Instr.Dr. Nurdan Saran

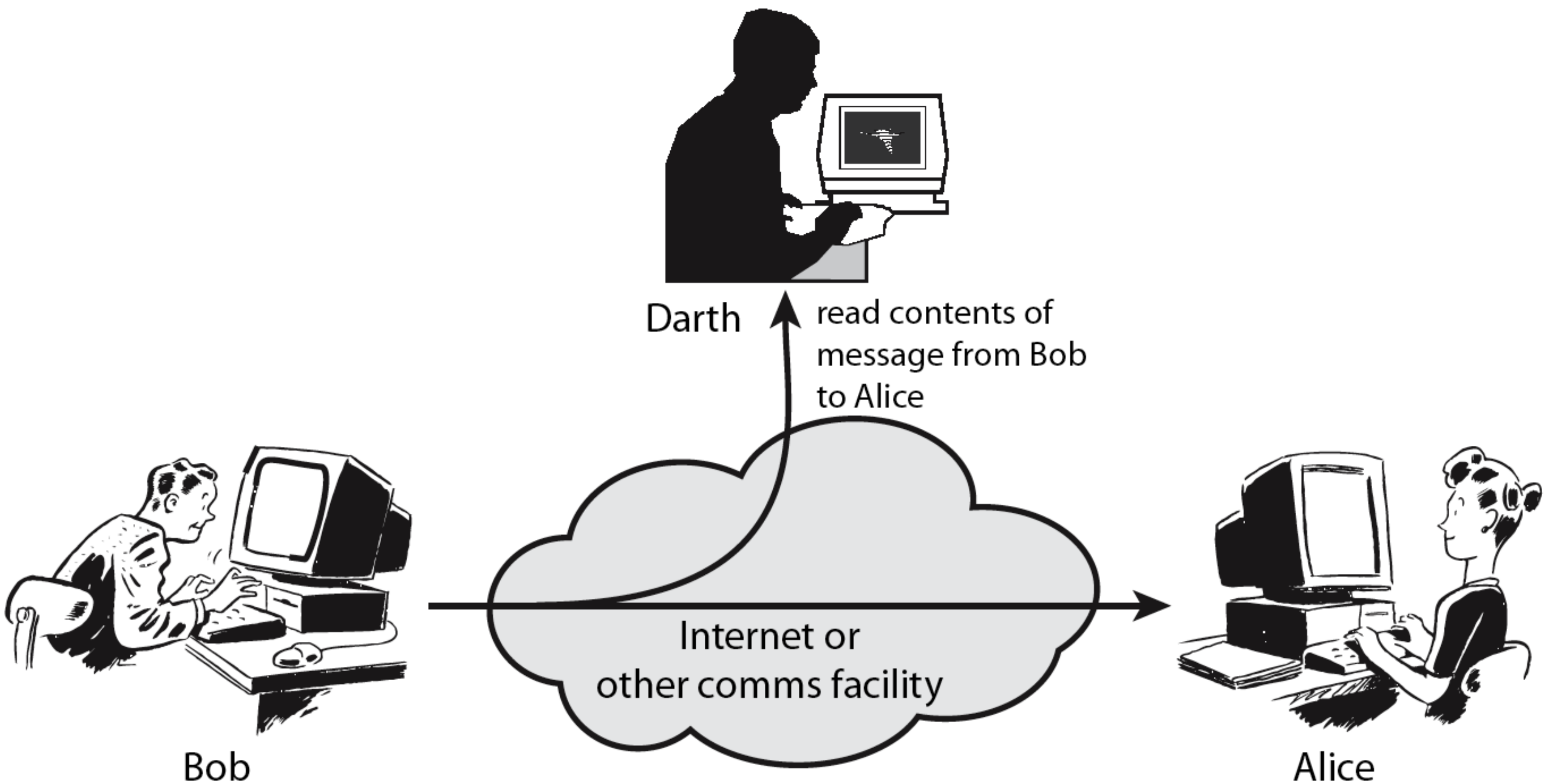
Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

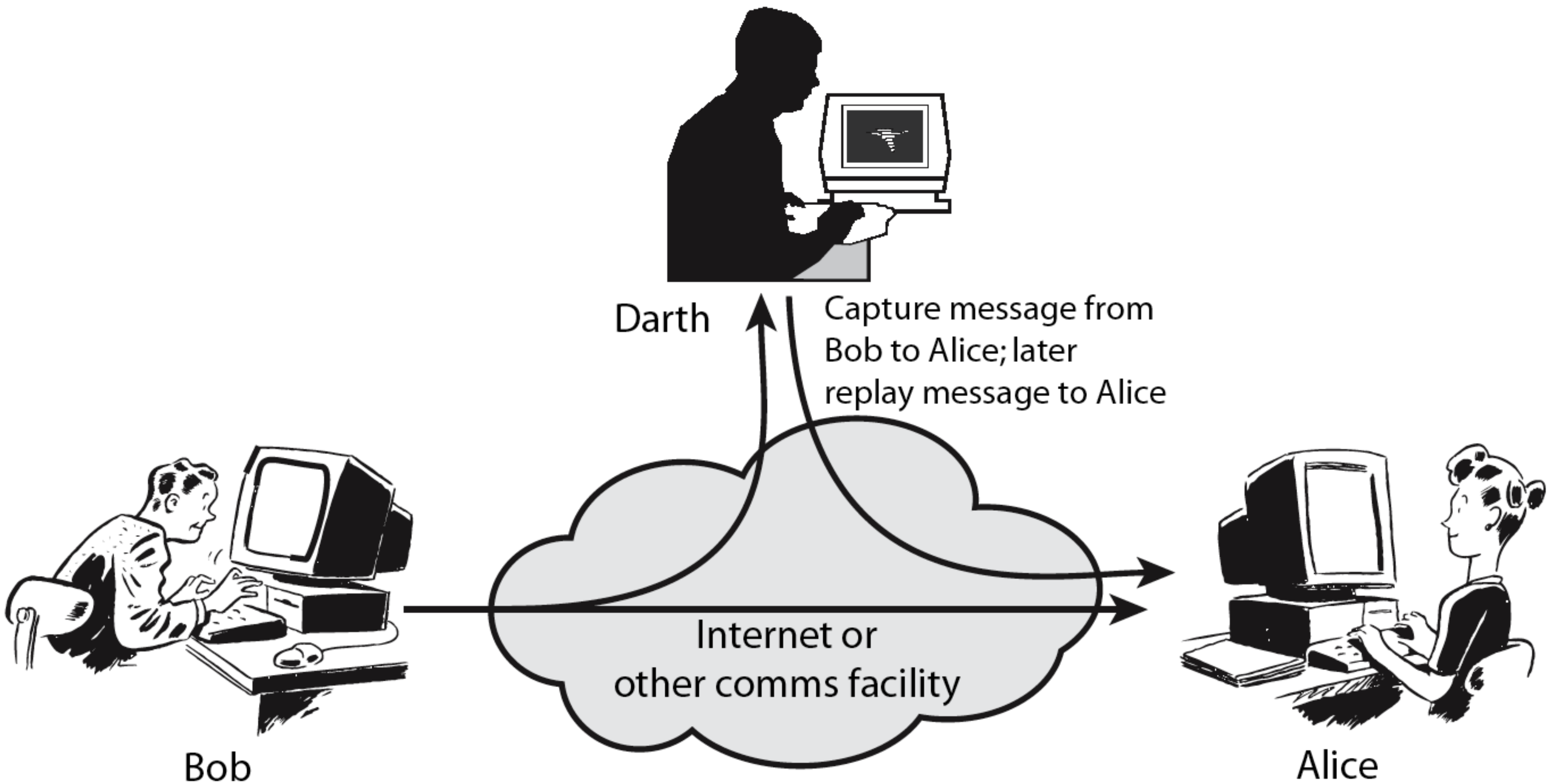
Security Attack

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing
- have a wide range of attacks
- can focus of generic types of attacks
  - passive
  - active

Passive Attacks



Active Attacks



Classify Security Attacks as

- **passive attacks** - eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
- **active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

Security Services

- **Privacy**
- **Authentication :** verifies the identity of the source
- **Data Integrity :** protects the data from modification
- **Non-repudiation :** prevent a party from denying previous actions or aggreements.
- **Confidentiality :** keep information secret to anyone but the intended recipients.

Greek:

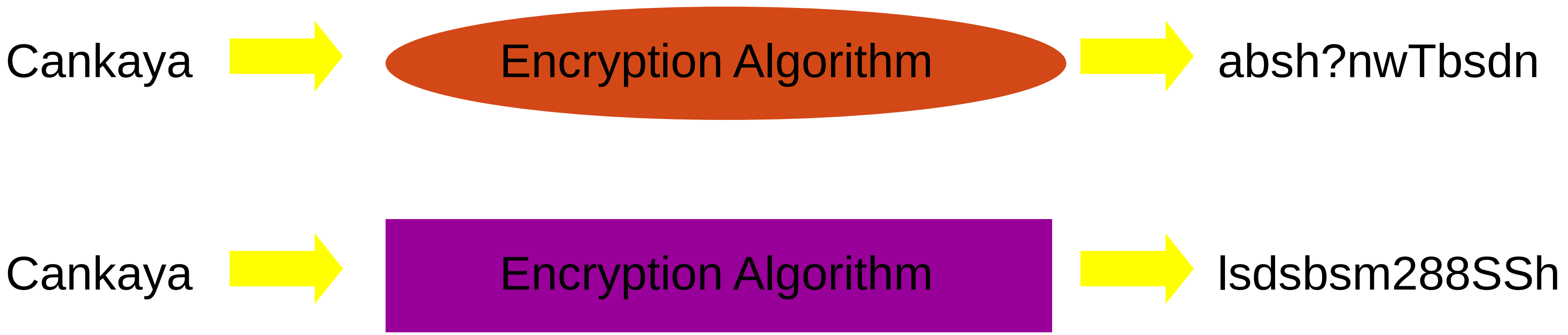
kryptos + graphein → hidden writing

Cryptography is the study of secret (crypto) writing (graphy) concerned with developing algorithms which may be used to

- conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or
- verify the correctness of a message to the recipient (authentication)
- form the basis of many technological solutions to computer and communications security problems

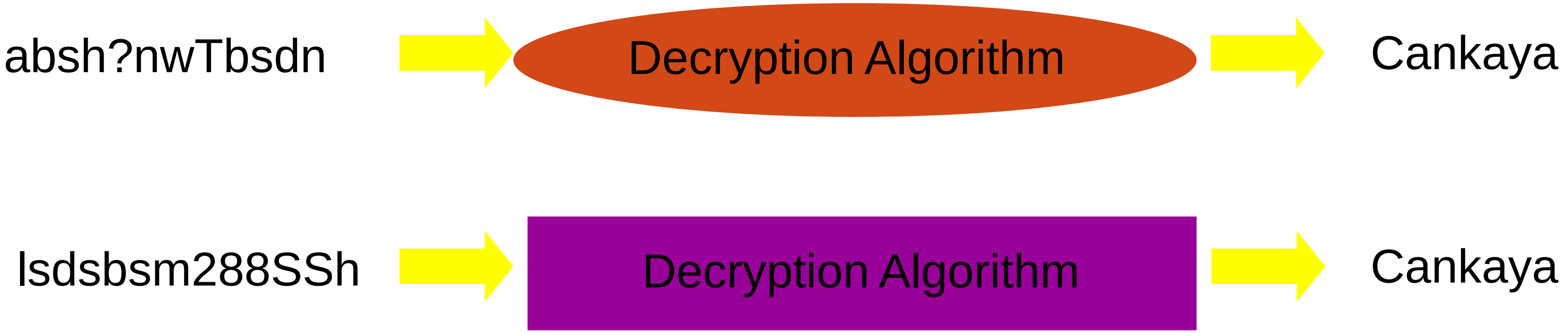
Encryption

- Convert normal, readable data into obscured, unreadable data



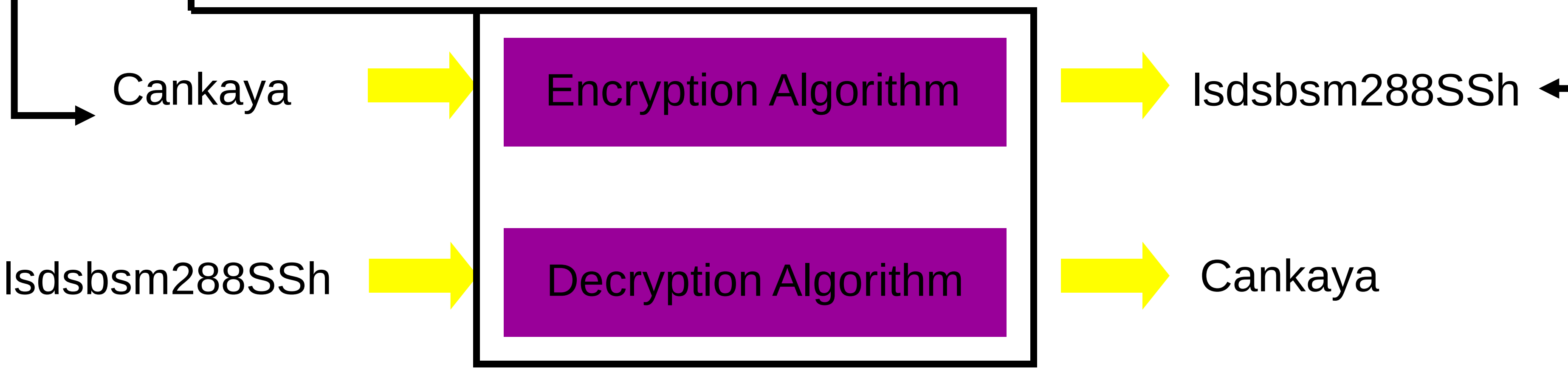
Decryption

- Convert obscured, unreadable data into normal, readable data



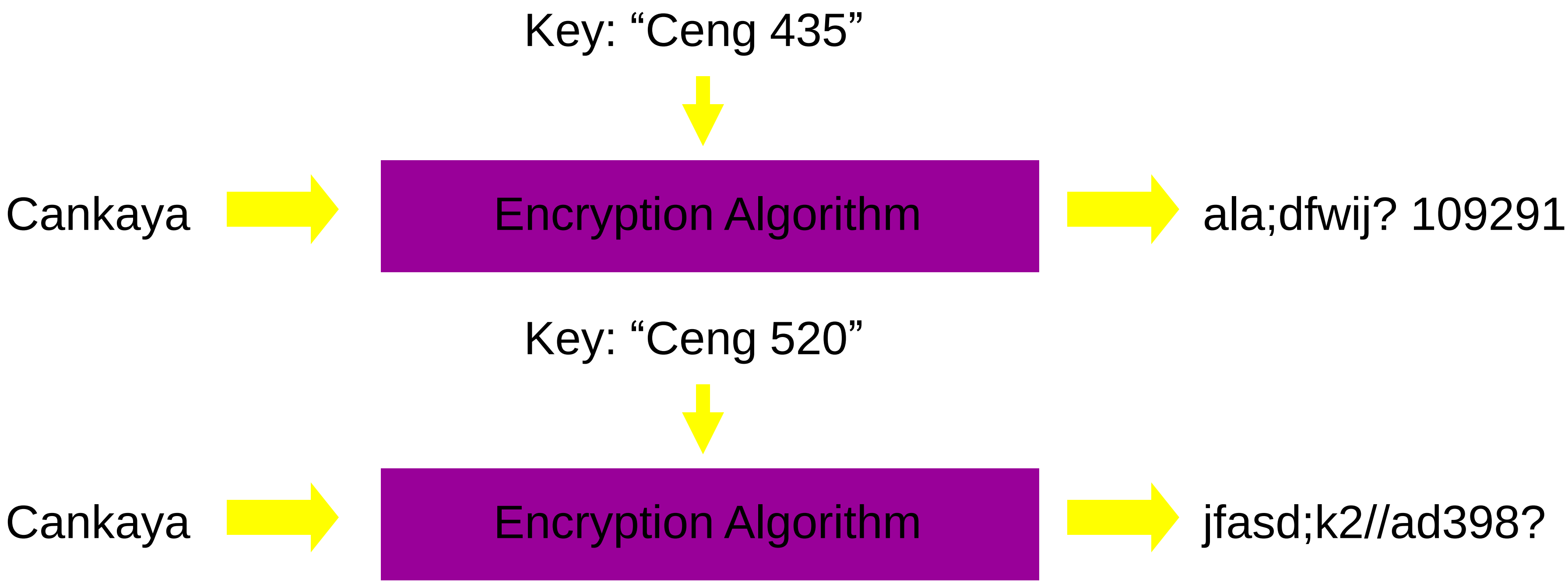
Terminology

- plaintext - clear readable text
- ciphertext - unreadable text
- cipher - algorithm(s) for encryption and decryption



Terminology

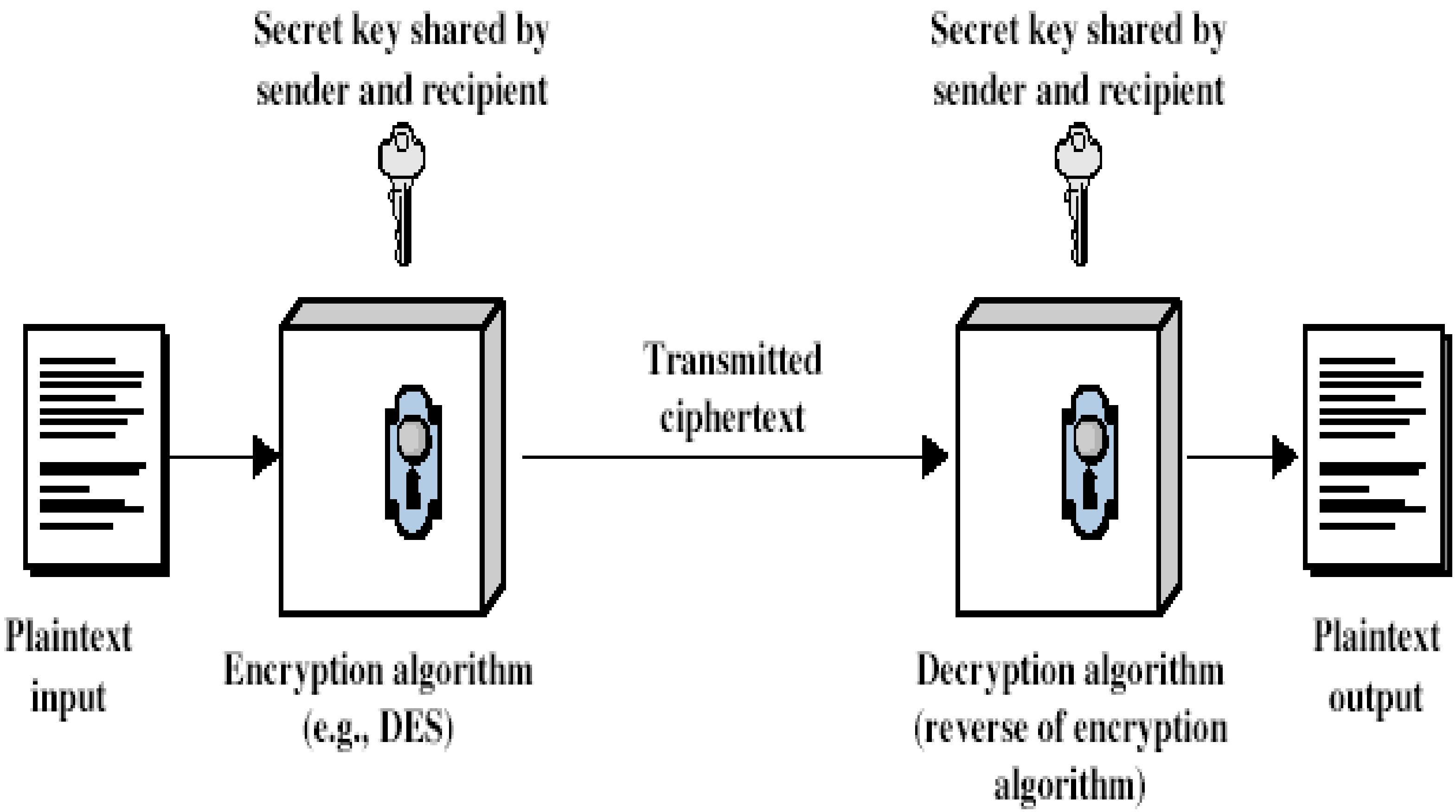
- Key -- a secret piece of information that controls how the encryption algorithm works
- Different keys produce different encrypted results



Symmetric Encryption

- or conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970's
- and by far most widely used

Symmetric Cipher Model



Symmetric Key

- Alice wants to send a private/confidential message to Bob
- Alice computes $c=E_k(p)$
- Sends c to Bob over unsecured wire
- Bob computes $p=D_k(c)$

Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- assume encryption algorithm is known
- implies a secure channel to distribute key
- Shared secret is great… but how do we distribute it?

Asymmetric Key Cryptography

- Instead of one key, have two
  - public key
  - private key
    - Use one key to encode/encrypt
    - Use other key to decode/decrypt
- Someone can know public key
- Computing private key from public key is very, very difficult (factoring huge number)

Application: Secrecy

- Bob has Bob.pub, Bob.priv
- Alice has Alice.pub, Alice.priv
- Alice wants to send Bob a secret "I Love You" note

Application: Secrecy

- Alice finds Bob.pub from his website
- Alice computes $c = E_{Bob.pub}(p)$
- Sends c to Bob over unsecured wire
- Bob computes $p = D_{Bob.priv}(c)$

Advantages

- Key distribution not a problem!
- Anyone can send a message to Bob
- Only Bob can decrypt!

Application: Authenticity

- Alice wants to tell Bob the message is really from her!
- Digital signature
- Alice computes $c = E_{Alice.priv}(p)$
- Alice sends c over unsecured wire
- Anyone can check that Alice is the sender… by computing $p = D_{Alice.pub}(c)$

Authenticity + Secrecy

Alice	Carl & Eve	Bob
A.priv	Bad People!	B.priv
	A.pub, B.pub, ...	
"I love you"		

Authenticity + Secrecy

Alice	Carl & Eve	Bob
A.priv	Bad People!	B.priv
	A.pub, B.pub, ...	
"I love you"		
B.pub		

Authenticity + Secrecy

Alice

A.priv

"I love you"

B.pub

"This is from A"

Carl & Eve

Bad People!

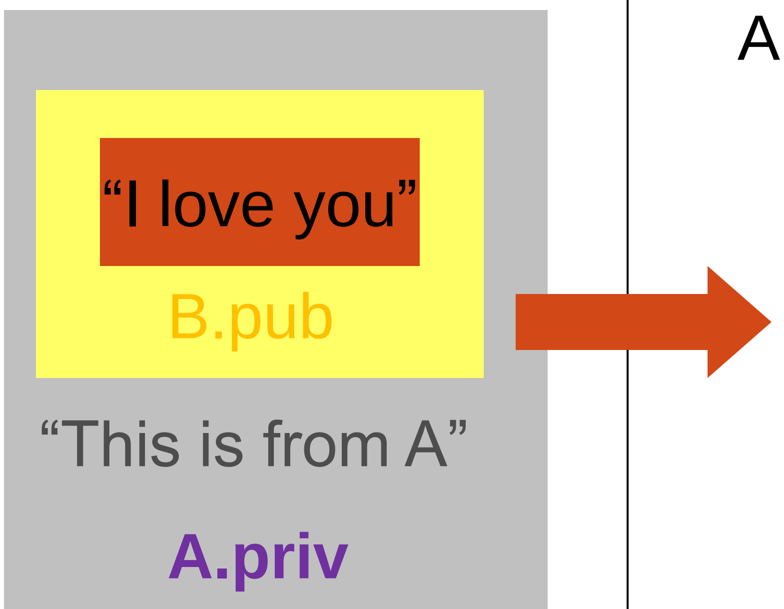
A.pub, B.pub, ...

Bob

B.priv

Authenticity + Secrecy

Alice	Carl & Eve	Bob
A.priv	Bad People!	B.priv
	A.pub, B.pub, ...	



Authenticity + Secrecy

Alice	Carl & Eve	Bob
A.priv	Bad People!	B.priv
	A.pub, B.pub, ...	

"I love you"

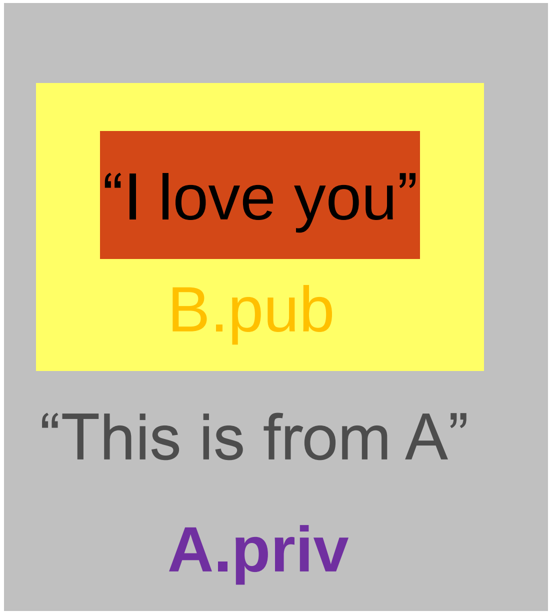
B.pub

"This is from A"

A.priv

Authenticity + Secrecy

Alice	Carl & Eve	Bob
A.priv	Bad People!	B.priv
	A.pub, B.pub, ...	



Hash Functions

- A **cryptographic hash function** is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string.
- h = hash(data)
- Every bit in input affects output
- Hash function is not invertible

Some properties of Hash Function

- it is easy to compute the hash value for any given message,
- it is infeasible to find a message that has a given hash,
- it is infeasible to modify a message without changing its hash,
- it is infeasible to find two different messages with the same hash.

Error Checking

- Alice wants to send a LONG message to Bob
- Alice computes h=hash($LONG_MSG);
- Sends data to Bob, includes relatively short h at the end of message
- Bob recomputes hash.
  - If match, great! Data's correct!
  - If not match, either hash or data was corrupted. Resend.

Authenticity + Secrecy

Alice	Carl & Eve	Bob
A.priv	Bad People!	B.priv
	A.pub, B.pub, …	
“I love you”		

Authenticity + Secrecy

Alice	Carl & Eve	Bob
A.priv	Bad People!	B.priv
	A.pub, B.pub, ...	
"I love you"		
hash("I love you ...") → 12fea90897bddc		

Authenticity + Secrecy

Alice	Carl & Eve	Bob
A.priv	Bad People!	B.priv
	A.pub, B.pub, ...	

"I love you"

"This is from A"

12fea90897bddc
A.priv

Authenticity + Secrecy

Alice
A.priv

"I love you"

"This is from A"

12fea90897bddc
A.priv

Bob.pub

Carl & Eve
Bad People!

A.pub, B.pub, ...

Bob
B.priv

Authenticity + Secrecy

Alice
A.priv

Carl & Eve
Bad People!

A.pub, B.pub, ...

“I love you”

“This is from A”

12fea90897bddc
A.priv

Bob.pub

Bob
B.priv

Authenticity + Secrecy

Alice
A.priv

Carl & Eve
Bad People!

A.pub, B.pub, ...

Bob
B.priv

"I love you"

"This is from A"

12fea90897bddc
A.priv

Bob.pub

Authenticity + Secrecy

Alice	Carl & Eve	Bob
A.priv	Bad People!	B.priv
	A.pub, B.pub, ...	
		"I love you"
		"This is from A"
		12fea90897bddc A.priv

Authenticity + Secrecy

Alice	Carl & Eve	Bob
A.priv	Bad People!	B.priv
	A.pub, B.pub, ...	"I love you"
		"This is from A"
		12fea90897bddc
		=?
		hash("I love you")

Symmetric vs. Asymmetric

- Symmetric faster but relies on shared secret
- Asymmetric slower but "solves" distribution-of-keys problem

Characterization of Cryptographic System

- type of encryption operations used
  - substitution / transposition / product
- number of keys used
  - single-key or private / two-key or public
- way in which plaintext is processed
  - block / stream

Important Properties

- the encryption and decryption functions are efficiently computable for all keys k, i.e., it should be relatively easy both to encrypt and decrypt, given the key, and
- it should computationally infeasible to decipher the ciphertext, i.e., an opponent upon seeing a ciphertext should be unable to determine either the key k that was used or the original plaintext string.
- Usually assume the cryptographic system is public, and only the key is secret information

Cryptanalysis

- objective to recover key not just message
- general approaches:
  - cryptanalytic attack
  - brute-force 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

More Definitions

- **unconditional security**
  - no matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- **computational security**
  - given limited computing resources (eg time needed for calculations is greater than age of universe), the cipher cannot be broken

Brute Force Search

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/µs	Time required at 10^6 decryptions/µs
32	$2^{32} = 4.3 \times 10^9$	2^{31} µs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} µs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} µs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} µs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} µs = 6.4×10^{12} years	6.4×10^6 years