

Lec – 3a

Introduction to

Assignment Project Exam Help
Cryptography
<https://powcoder.com>

Add WeChat powcoder

Overview

- Security vs Cryptography
- Key terminologies
- CIA and Cryptography
- Algorithms/Ciphers and Keys
- Kerchoff's principle
- Secret key or symmetric cryptography Drawbacks
- Ring puzzle
- Public key or asymmetric cryptography

Assignment Project Exam Help

<https://powcoder.com>

Adel WeChat powcoder

Principles – CIA + AA



Information system assets



Assignment Project Exam Help
Malware

<https://powcoder.com>



Add WeChat powcoder

- Authentication is the first line of defence,
(will be covering password policies later)
- Cryptography used in authentication

Security vs Cryptography

- What is cryptography? The science of secret writing
- What is security ? Protect systems against inappropriate use.
Examples:
 - Withdraw money from someone else's account
 - Alter your exam marks on the university database
- Security is a broad subject; physical, platform, network,...
- Cryptography security; cryptography is only one way of ensuring certain aspects of security
- Every system can be broken (given enough resources) Security cost should be proportional to value being protected

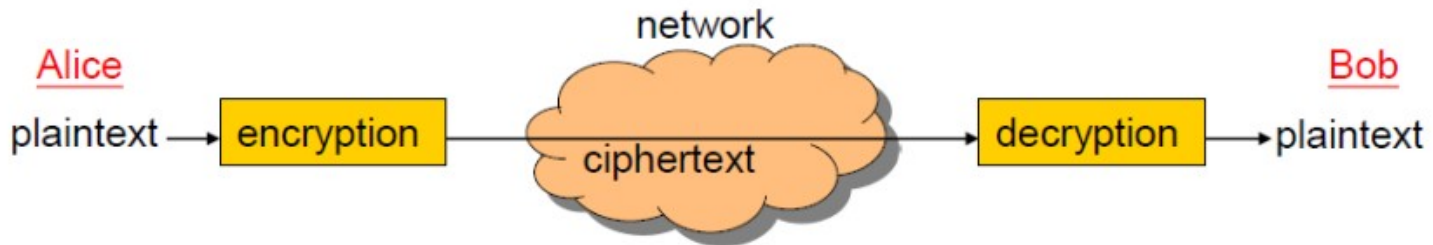
Some Terminologies

- Cryptography: the science of secret writing
- Cryptanalysis: the science of code-breaking
- Cryptology = Cryptography + Cryptanalysis
- A cipher is an algorithm that turns readable messages (plaintext) into unreadable messages (ciphertext). This process is called encryption. The reverse process is called decryption

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



Brief overview of crypto

- Algorithm - A finite sequence of well-defined, computer-implementable instructions, typically to solve a problem
- Ciphers are algorithms
- A cipher 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 private/symmetric key cryptosystem uses the same key to encrypt as to decrypt
- A public/asymmetric key cryptosystem uses a public key to encrypt and a private key to decrypt

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Basic idea of encryption / decryption

- Caesar, 2000 years ago

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Assignment Project Exam Help

- Suppose we know, <https://powcoder.com> has been used in this example and it is a shift by three characters

Given ciphertext: VSRQJH

Plaintext: sponge

Shift by n for some $n \in \{0, 1, 2, \dots, 25\}$

Then key is n

Example: key $n = 2$

Ciphertext: uwuugz plaintext

Another simple cipher is: Rot13

Replace every letter with the letter 13 places down the alphabet

Example: hello world → uryyb jbeyq

How to decrypt “qrpelcg” ?

Assignment Project Exam Help

Rot13 is not a good cipher, why?

<https://powcoder.com>

If an attacker knows Rot13 is being used, the message can easily be decoded

Add WeChat powcoder

What about Rot-n? (shift n positions)

Better

But still easy to decode (try all 26 values of n)

Algorithms & Keys

- Ciphers usually use keys
- Key is a secret value
- One algorithm, many different keys
- Encrypting the same plaintext using different keys (but the same algorithm) gives different ciphertexts
- Ciphertext can only be decrypted using the correct key (using an incorrect key decrypts into a mess)
- Only the key need to be kept secret (algorithm can be publicly known; see next slide)
- Example: in Rot-n, the value of n is the key 26 different possible keys

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Kerchoff's principle

Assignment Project Exam Help

A **cryptographic** system should be secure even if everything about the system, except the key, is public knowledge

<https://powcoder.com>

Add WeChat powcoder

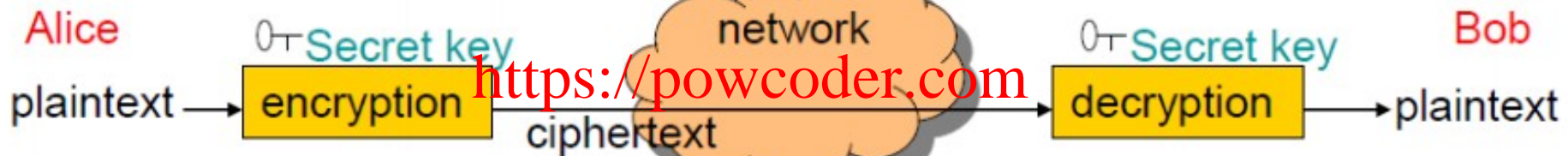
Secret / Symmetric key cryptography

- Also called symmetric cryptography
- Since ancient times
- Same key for encryption and decryption (to be kept secret)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



A generic view of symmetric key crypto

Symmetric

Analogy: locked box

To send a secret letter/Diamond, Alice locks it in a box and sends the locked box to Bob. Only Alice and Bob have the key to open the box

Think about , how Alice needs to send the secret key in a secure way?

Options: Post, Special Jet, Commercially these options are not viable.

Problems in Secret/Symmetric key cryptography

1) Key Distribution Problem – A drawback in symmetric

Keys are usually shorter than the message and can be reused. Still, it is difficult to distribute keys securely

2) In a system with many components:

Using one key for everything: risk the whole system collapsing upon a security breach

Use a (different) key for each pair: distribution headache

Solution to key distribution problem: key agreement protocols; public key cryptography

Symmetric ciphers


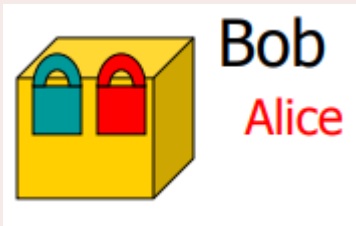


- AES (Advanced **Encryption** Standard)
- DES (Data **Encryption** Standard)
- 3DES (Triple **DES**)
- IDEA (International Data **Encryption** Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest **Cipher** 4)
- RC5 (Rivest **Cipher** 5)
- RC6 (Rivest **Cipher** 6)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

A possible solution to key distribution

Bob		Alice
	Bob puts the letter / diamond ring inside the box, put his lock and sends it Alice	
<div>Assignment Project Exam Help</div> <div>https://powcoder.com</div> <div>Add WeChat powcoder</div>		
	Alice receives the box and puts another lock on it and sends the double locked box back to Bob	
	Bob removes his lock and sends the (still locked) box to Alice	
	Alice opens her lock and gets the secret letter / ring	

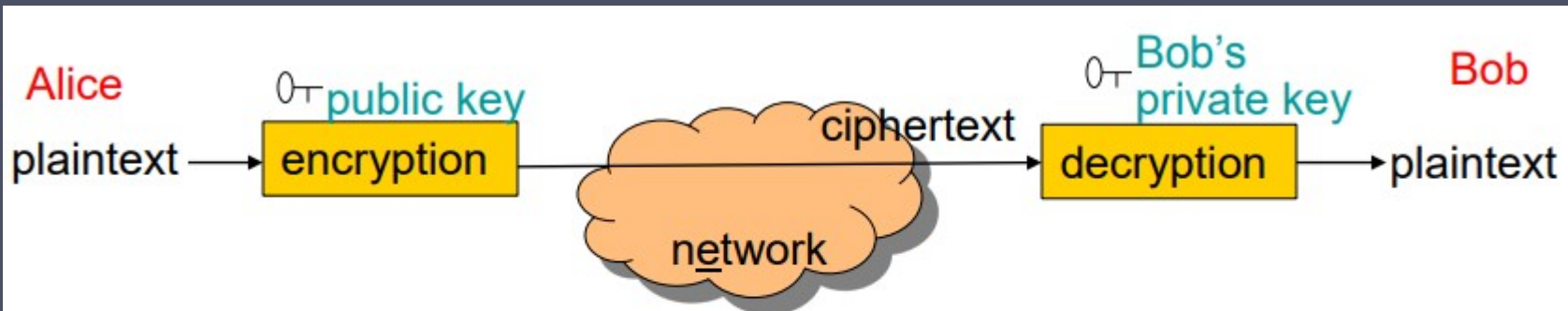
Asymmetric / Public key cryptography

- Suppose Alice wants to send Bob a message
- Bob generated his keypair before hand
- Alice encrypts the message using Bob's public key
- Bob decrypts the message using his own private key
- Only Bob can decrypt the message since only he has his own private key

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



- No need for distributing a secret key
- Drawback: slow

Properties of Public and Private Keys

We need the following mathematical properties:

- Easy to generate a pair of public/private keys
 - Easy to encrypt knowing the public key
 - Easy to decrypt knowing the private key
 - Computationally difficult to get the private key from the public key
 - Computationally difficult to decrypt without knowing the private key
- <https://powcoder.com>
- Add WeChat powcoder
- (Preferably) can encrypt with private key and decrypt with public key (i.e. key roles exchanged)

Is there really such a nice thing?

Some mathematical problems are believed to have these properties

Asymmetric ciphers examples

- RSA
- El Gamal
- Diffie-Hellman
- Elliptic curve cryptography – used in Bitcoins

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Hybrid systems

- Combines symmetric and asymmetric ciphers
- First, the two parties use an asymmetric cipher to negotiate a session key(a secret key for this conversation)

Assignment Project Exam Help

Then, encrypt the conversation using the session key as a secret key of a symmetric cipher

<https://powcoder.com>

Add WeChat powcoder

Combines virtues of both kinds of ciphers:

- Use the slow asymmetric cipher to exchange a small amount of data only
- The conversation can then be encrypted using a fast-symmetric cipher

Concepts of cipher attacks

- “Breaking” a cipher means decrypt plaintext without the key
- Possible when plaintext language has some “meaning” for attacks to be possible

e.g. English sentences, excel file, exe program, ...

Otherwise, no way to distinguish correct or incorrect decryption

<https://powcoder.com>

Two types of attacks on ciphers:

- Brute-force
- Cryptanalysis

Note: breaking a cipher is not the only way of compromising the cryptosystem

Brute force attack

Try all possible keys, one by one

- Strength of cipher can be increased by using longer keys
- E.g. Rot-n having only 26 possible keys is too small
- An n -bit key length gives 2^n different possible keys

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Cryptanalysis

- Exploit the mathematical properties of the algorithm
- Strength of cipher depends on design of algorithm
- Secret key ciphers: cryptanalysis is possible if structure (statistical properties) of plaintext remains in ciphertext
- Public key ciphers: cryptanalysis usually focuses on the mathematical relationships between public and private keys
- “Perfect” cipher does not admit cryptanalysis is better than brute force

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Types of cryptanalysis attack

Type of Attack	Known to Cryptanalyst
Ciphertext only	<ul style="list-style-type: none">•Encryption algorithm•Ciphertext to be decoded
Known plaintext	<ul style="list-style-type: none">•Encryption algorithm•Ciphertext to be decoded•One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	<ul style="list-style-type: none">•Encryption algorithm•Ciphertext to be decoded•Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	<ul style="list-style-type: none">•Encryption algorithm•Ciphertext to be decoded•Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	<ul style="list-style-type: none">•Encryption algorithm•Ciphertext to be decoded•Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key•Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Types of cryptanalysis attack examples

Ciphertext-only: only have (a large amount of) encrypted data

Example: Sgd pthbj agnvm enw itl Dr nvdg sgd karyx cif = ?

Known plaintext: in addition, some plaintext-ciphertext pairs are known

Example: Sgd = The, enl = dog, pthbj agnvm enw = ?

Email headers, guessed keywords in message, etc

Chosen plaintext: attacker can choose to encrypt a few plaintext

Example: Encrypt "Example"? => Dwzlok d

Cryptography

Classified along three independent dimensions.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The type of operations used for transforming plaintext to ciphertext

- Substitution – each element in the plaintext is mapped into another element
- Transposition – elements in plaintext are rearranged

The number of keys used

- Sender and receiver use same key – symmetric
- Sender and receiver each use a different key - asymmetric

The way in which the plaintext is processed

- Block cipher – processes input one block of elements at a time
- Stream cipher – processes the input elements continuously