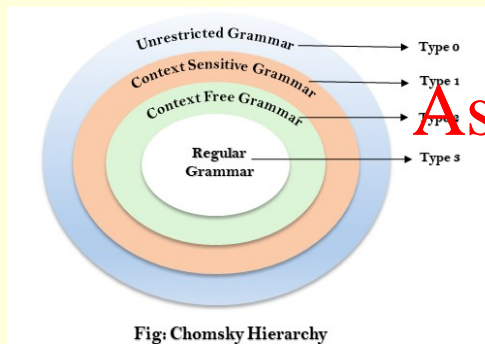


COSC1107 Computing Theory

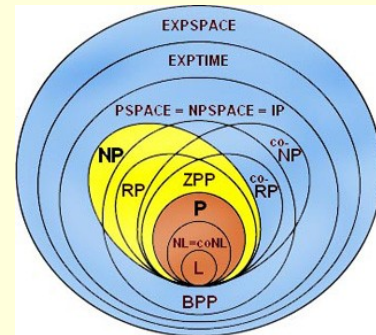
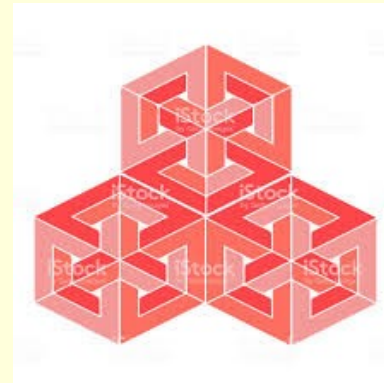
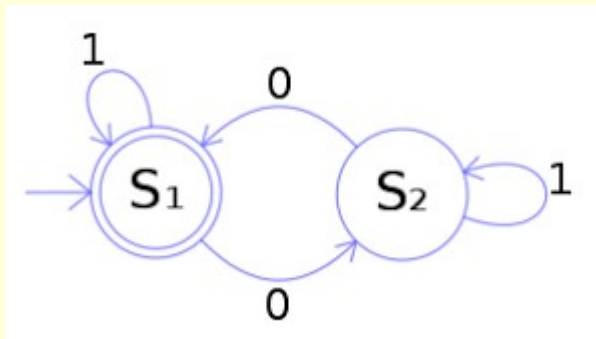
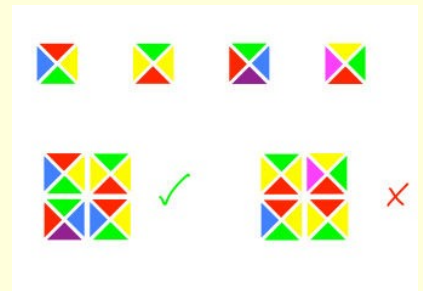
(We will commence soon. We are just allowing a few minutes for people to join and set up. *Please mute your microphone unless you are speaking.* You can raise your hand or use the chat at any time.)

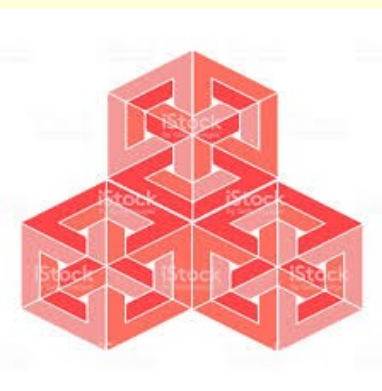
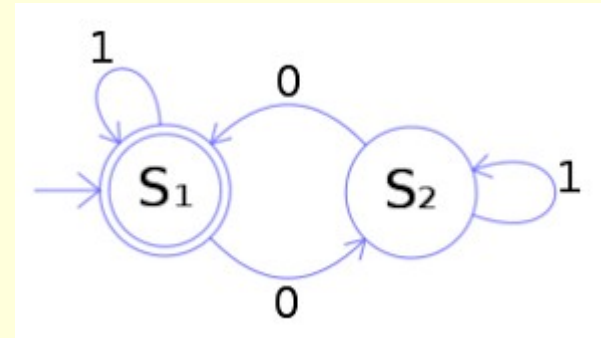
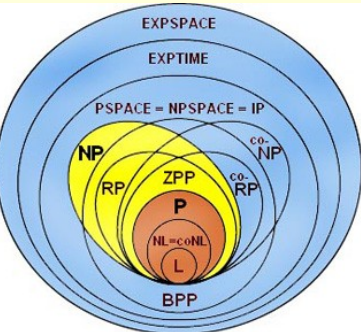


Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder





COSC1107
Assignment Project Exam Help

Computing Theory

<https://powecoder.com>

Zero-knowledge Proofs

Add WeChat powecoder

Week 11

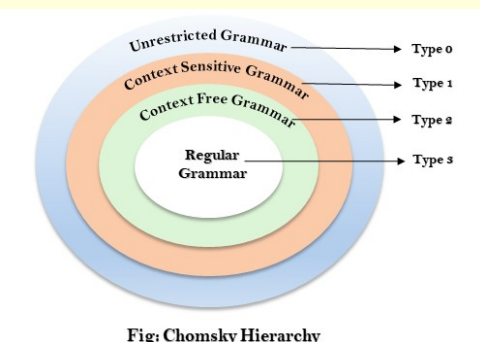
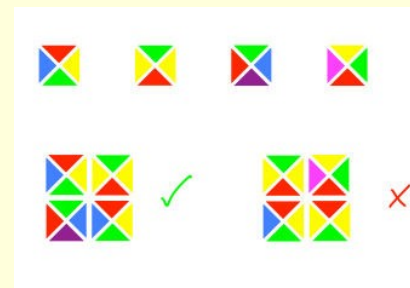


Fig: Chomsky Hierarchy

James Harland

james.harland@rmit.edu.au

* With thanks to Sebastian Sardina

Intro music 'Far Over' playing now ...



Week 11

Computing Theory

Acknowledgement



RMIT University acknowledges the people of the Woi wurrung and Boon wurrung language groups of the eastern Kulin Nations on whose unceded lands we conduct the business of the University. RMIT University respectfully acknowledges their Ancestors and Elders, past and present.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

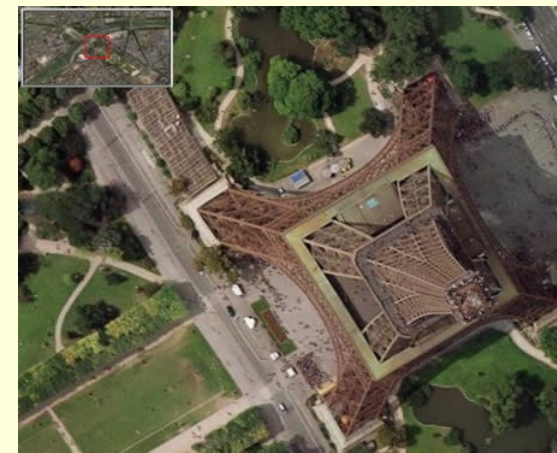
RMIT also acknowledges the Traditional Custodians and their Ancestors of the lands and waters across Australia where we conduct our business.

(add your name [here](#) to volunteer for this or email me)

(my personal Acknowledgement of Country is [here](#))

Overview

- Questions?
- Authentication
- Questions? Assignment Project Exam Help
- Secure dealings
- Questions? <https://powcoder.com>
- Zero-knowledge proofs Add WeChat powcoder
- Questions?
- Platypus Game
- Questions?



Weekly Schedule



	Lecture/Lectorial	Tutorial	Assessment
1	Formal languages, grammars	Motivations & Mathematical preliminaries	
2	Finite State Machines	Grammars	Quiz 1
3	Pushdown Automata, nondeterminism	NFAs and DFAs	Quiz 2
4	Turing machines	Pushdown automata	Quiz 3
5	Computability, universality	Turing machines	Quiz 4
6	Pumping Lemma, NFA \rightarrow DFA conversion	Computability, universality	Assignment 1, Quiz 5
7	Chomsky Hierarchy	Nondeterminism, Pumping Lemma	Quiz 6
8	Unrestricted grammars		Quiz 7
9	Complexity and intractability	Unrestricted grammars	Quiz 8
10	NP-completeness	Complexity and intractability	Quiz 9
11	Zero-knowledge proofs	NP-completeness	Quiz 10
12	Research and requests	Sample exercise	Assignment 2
14-16	--	--	Final exercise

Foundations

Relationships

Analysis

Assessment

Week 11

Computing Theory

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Weekly Schedule



	Lectorial	Tutorial	Assessment
11	Zero-knowledge proofs	NP-completeness	Quiz 10
12	Research and requests	Sample exercise	Assignment 2
14-16	--	Assignment Project Exam Help	Final exercise

<https://powcoder.com>

- Send me requests for Week 12 class by **Friday 8th October**
Add WeChat powcoder
- Some parts of Assignment 2 will be submitted **online**
- Sample exercise will be in tutorials next week
- Information about all of these will be announced on Ed

Questions?



Questions?



Assignment Project Exam Help

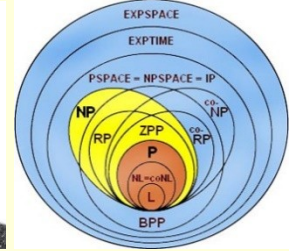
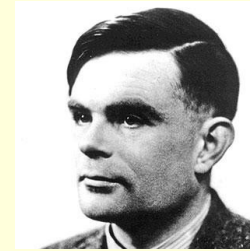
<https://powcoder.com>

Add WeChat powcoder

Questions?



Encryption



"Bob sucks!
From Alice"



Encrypt



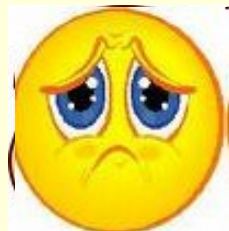
xsgf
hasf
gedg

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Send



"Bob sucks!
From Alice"

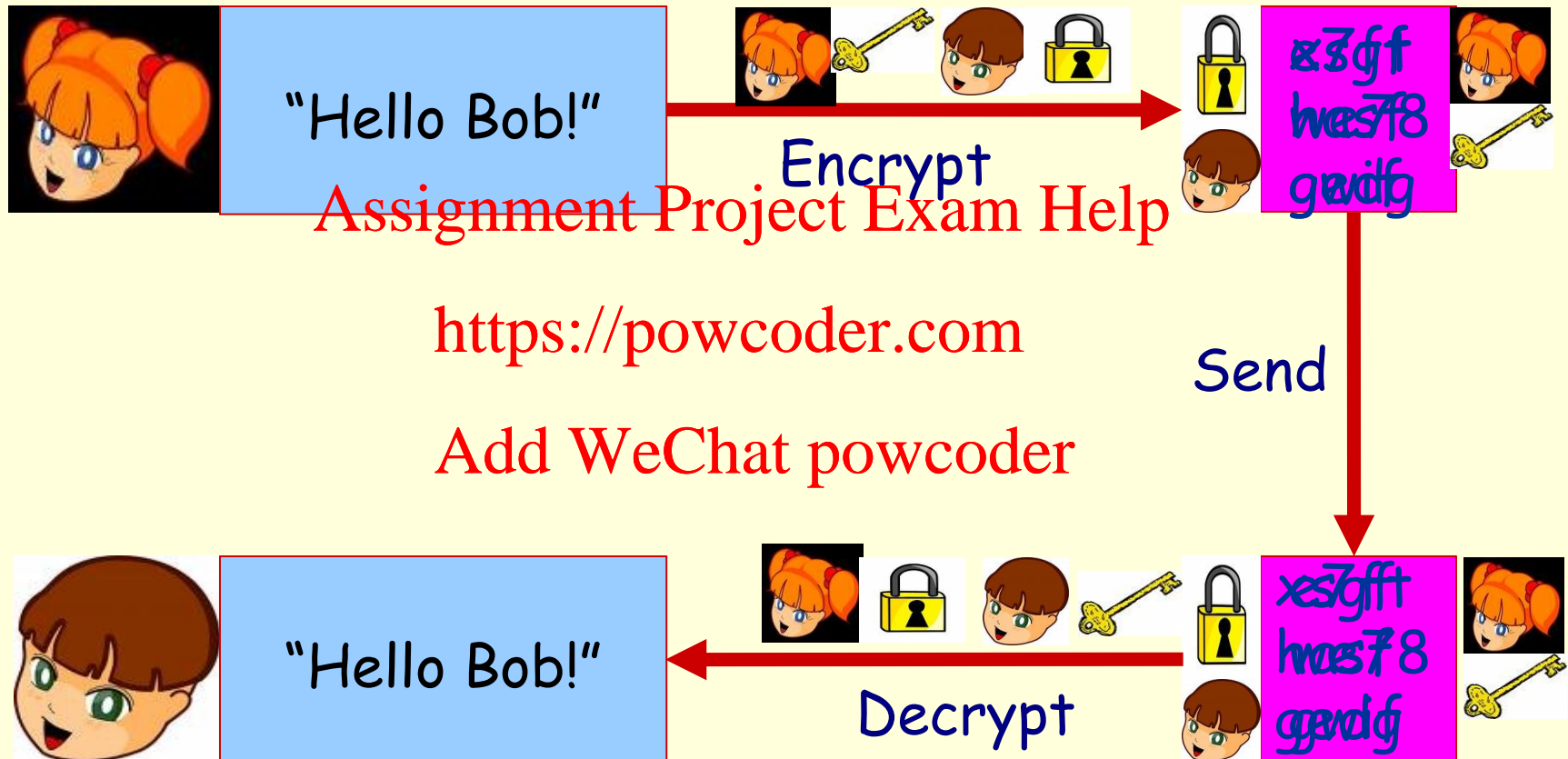
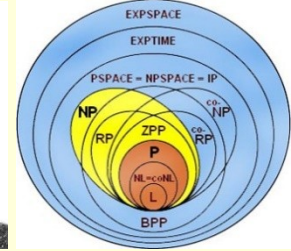
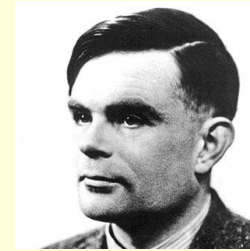


Decrypt



xsgf
hasf
gedg

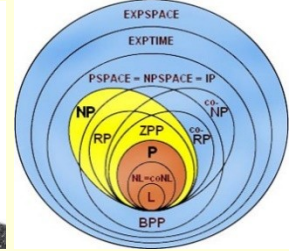
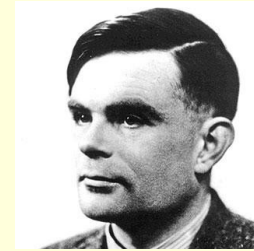
Encryption



<https://powcoder.com>

Add WeChat powcoder

Authentication

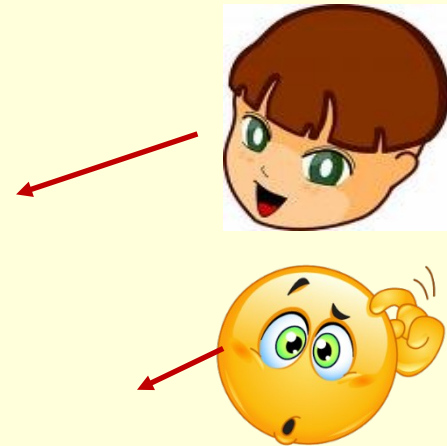


- Alice sends $m' = E_B(D_A(m))$ to Bob
- Bob decodes message with $E_A(D_B(m'))$
- Bob sees $E_A(D_B(E_B(D_A(m)))) = E_A(D_A(m)) = m$
- Spy message arrives as $m' = E_B(m)$
- Bob decodes with $E_A(D_B(E_B(m))) = E_A(m)$
- Alice's messages could only have been sent by Alice (as only Alice knows D_A)
- Spy message could have been sent by anyone (including Alice)

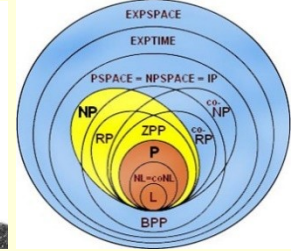
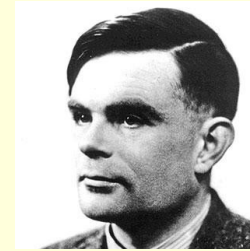
Assignment Project Exam Help

<https://powcoder.com>

Add WeChat: powcoder



Authentication



- This can be done with any public-key scheme for which
 - $D(E(m)) = E(D(m))$
 - RSA satisfies this (ie order of decryption and encryption doesn't matter)
- Can also be useful to have
 - $E_A(E_B(m)) = E_B(E_A(m))$ (and same for decryption)
 - RSA satisfies this too (ie order of encryption and/or decryption doesn't matter)

Questions?



Questions?



Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Questions?



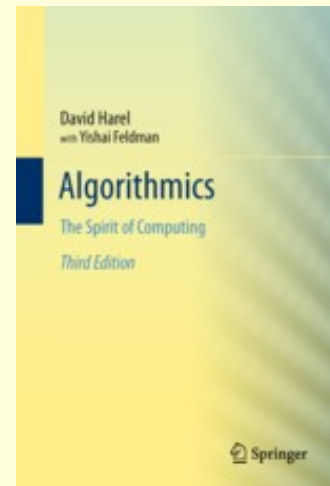
Secure Dealings



Who does the dealing?

- No central 'umpire'
- No-one trusts anyone
- Need to distribute cards which are hidden
- Need to be able to authenticate card distribution
- Online equivalent of 'you cut, I'll shuffle'

Great reference: David Harel & Yishai Feldman, Algorithmics (3rd edition), Springer, 2012. (especially Chapter 12)



Secure Dealings



Alice shuffles



Bob discards 2, chooses 2 others, sends rest to Alice

Assignment Project Exam Help



Shuffles



<https://powcoder.com>

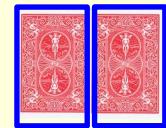
Add WeChat powcoder



discards 2, chooses 2



How do we implement 'face down'?



Secure Dealings



1,2,3,4,5,6

Shuffles, encrypts

$E_A(4,1,2,5,3,6)$



Assignment Project Exam Help



<https://powcoder.com> cards 2, encrypts 2

$E_A(4,5), E_A(E_A(2,3))$
Add WeChat powcoder

decrypts all

4,5

$E_B(2,3)$

decrypts
2,3

Secure Dealings



- Deal 2 cards each from a deck of 6 to 2 players A and B
- All keys kept secret (until after game)**
- 1,2,3,4,5,6 original Project Exam Help
- $E_A(4,1,2,5,3,6)$ A shuffles and encrypts all cards
<https://powcoder.com>
- $E_A(4,5) E_B(E_A(2,3))$ B chooses 4, encrypts 2
Add WeChat powcoder
- 4,5, $E_B(2,3)$ A decrypts all 4
- $E_B(2,3)$ A sends encrypted cards to B
- 2,3 B decrypts

Secure Dealings



- Bob doesn't know which cards Alice has
- Alice doesn't know which cards Bob has
- Afterwards, they can exchange decryption keys
- Bob can check $E_A(4,1,2,5,3,6)$
- Alice can check $E_B(E_A(2,3))$ and $E_B(2,3)$
- No-one gets shot :-)

Questions?



Questions?



Assignment Project Exam Help

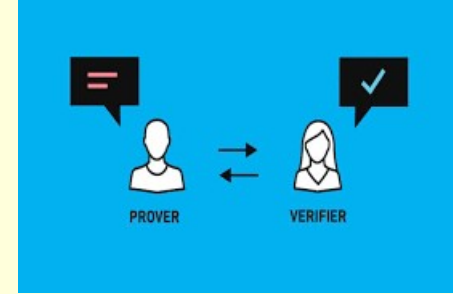
<https://powcoder.com>

Add WeChat powcoder

Questions?



Zero-knowledge Proofs



Question: How can you prove that you know a secret without revealing it?

What is your PIN?

Password:

First pet?

Assignment Project Exam Help

Answer: Probabilistically (!!)

<https://powcoder.com>



Add WeChat powcoder



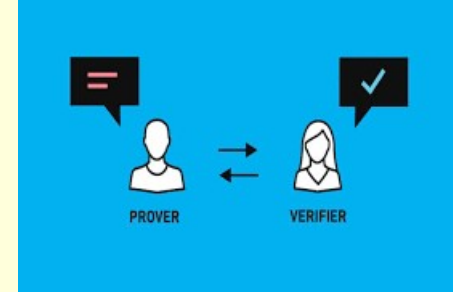
"I know the secret!"

prover

"Convince me!"

verifier or doubter

Zero-knowledge Proofs



- NP-complete problems are useful here:
- Solution can be **checked** in polynomial time
- (Almost certainly) solution can't be **found** in polynomial time

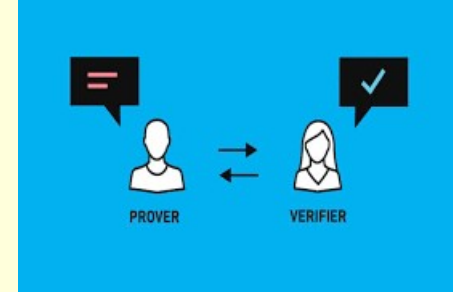
<https://powcoder.com>

Add WeChat powcoder

We use a **probabilistic** version of **checking a solution**

Usually **interactive** as well

Zero-knowledge proofs



Prover is often known as 'Peggy'

Verifier is often known as 'Victor'

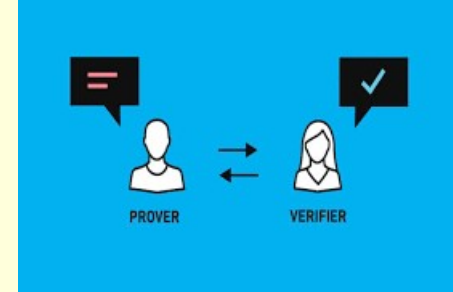


Assumptions: <https://powcoder.com>

Add WeChat powcoder

- Peggy and Victor are both rational and sincere
- Peggy only needs to convince Victor
- Victor does not know the secret
- Victor will only allow access if he is convinced
- Peggy and Victor act independently and don't collude
- Peggy reacts to input from Victor
- Process continues until Victor is convinced or claim is disproved
- Peggy's 'proof' **must not allow Victor to know the secret**

Zero-knowledge proofs



"I know the secret!"

"Do this then!"

Assignment Project Exam Help

(performs action successfully)

<https://powcoder.com>

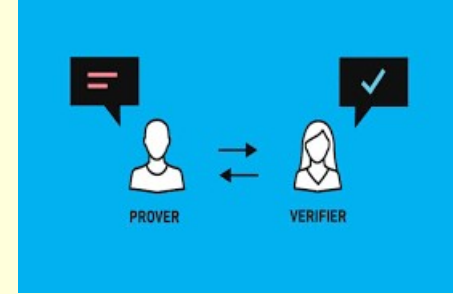
"Okay. Now do this!"

Add WeChat powcoder

(performs action unsuccessfully)

"GOTCHA!"

Zero-knowledge proofs



"I know the secret!"

"Do this then!"

(performs action successfully)
Assignment Project Exam Help

"Okay. Now do this!"
<https://powcoder.com>

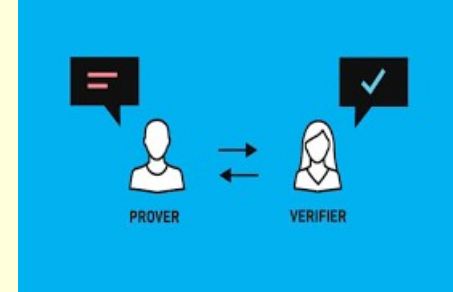
(performs action successfully)
Add WeChat powcoder

"Okay. Now do this!"

(performs action successfully)

"Ok! I am convinced."

Ali Baba example



Exit A



"?"

Door A

Entrance

Door B



Assignment Project Exam Help

Exactly one of Door A and Door B is open at any time

<https://powcoder.com>

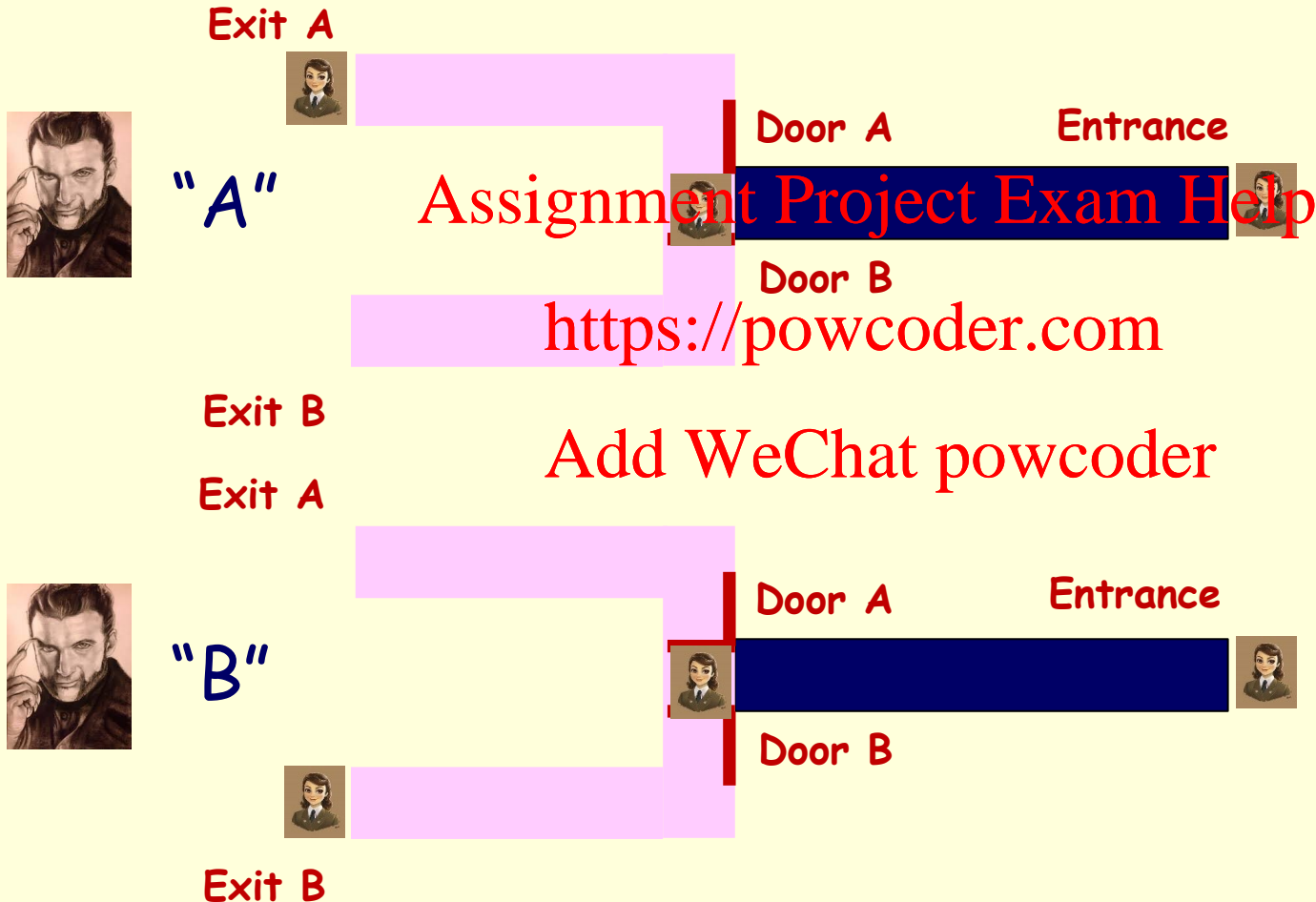
Exit B

Action:

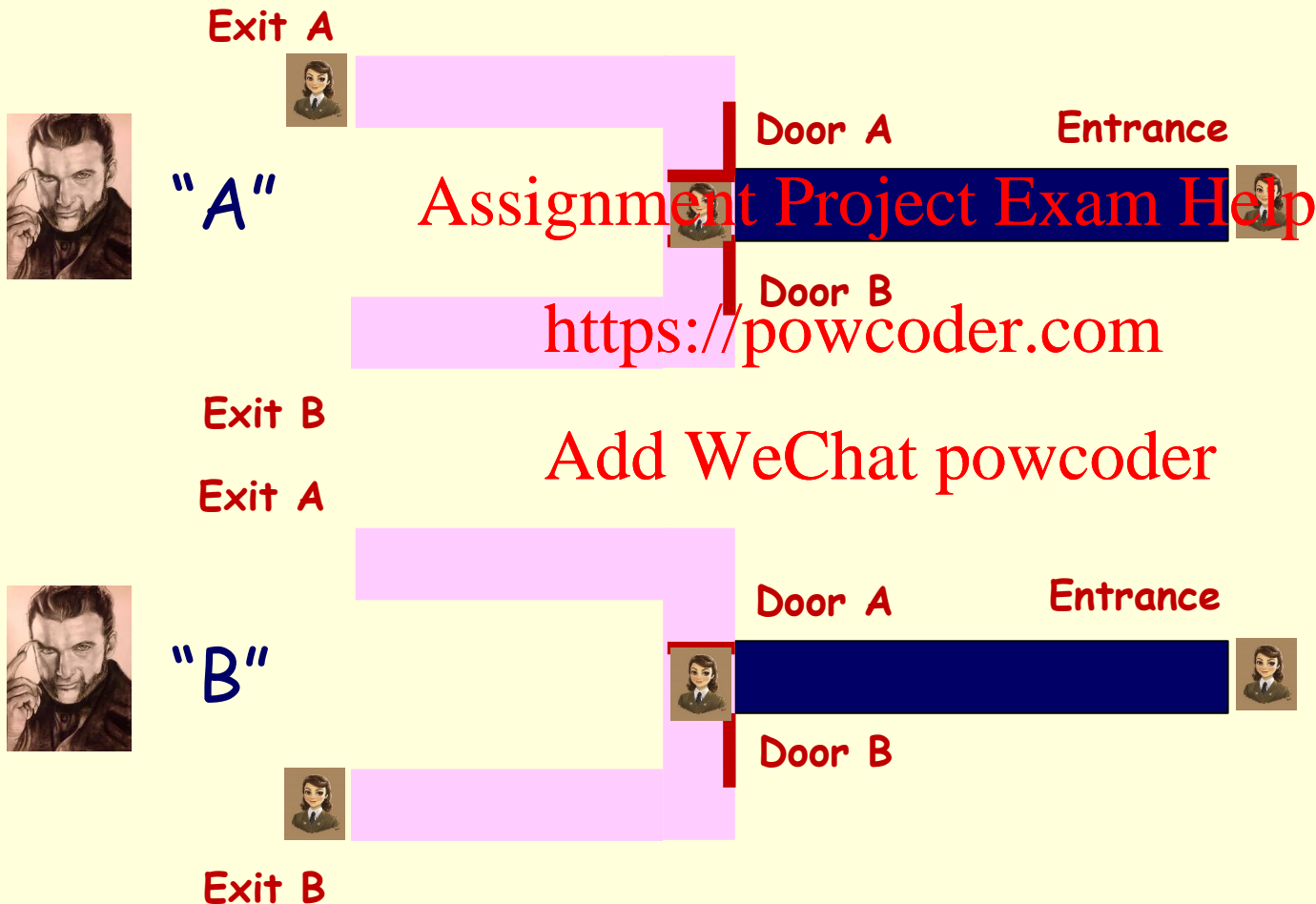
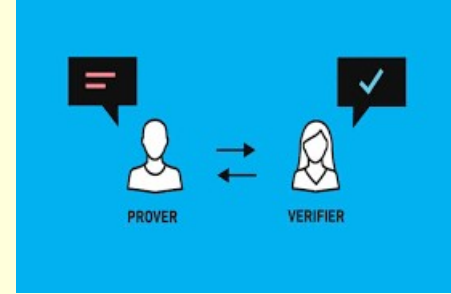
Add WeChat [powcoder](https://powcoder.com)

- Peggy goes into the tunnel
 - Victor randomly chooses an exit
 - Peggy then comes out Exit A or B
 - Successful if **Peggy is at the exit Victor chose**
- How to open either door
(or how to 'flip' the doors' status)

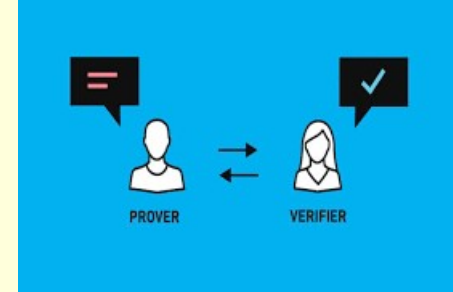
From: Jean-Jacques Quisquater, Louis Guillou & Thomas Berson, "How to Explain Zero-Knowledge Protocols to Your Children", Advances in Cryptology - CRYPTO'09, LNCS 435 628-631, 1990.



Ali Baba example



Ali Baba example



"?"

Exit A

Door A

Entrance

Door B

Exit B

Assignment Project Exam Help

Exactly one of Door A and Door B is open at any time

<https://powcoder.com>

For n trials:

Probability of passing 1 test falsely is $(1/2)$

Probability of passing 2 tests falsely is $(1/2)^2$

Probability of passing 3 tests falsely is $(1/2)^3$

...

Probability of passing n tests falsely is $(1/2)^n$

When $n = 20$, this is 0.0000009536 (!!) (99.9999046% correct)

Questions?



Questions?



Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Questions?



Quiz time!

Go to **Canvas** and find the quiz **Lectorial 11 Question set**

- Not worth any marks
- You can consult other students if you wish
- Time limit will be **5** minutes

Assignment Project Exam Help

<https://powcoder.com>



Week 10



Computing Theory

Go!

The pictures will take 5 minutes to disappear!

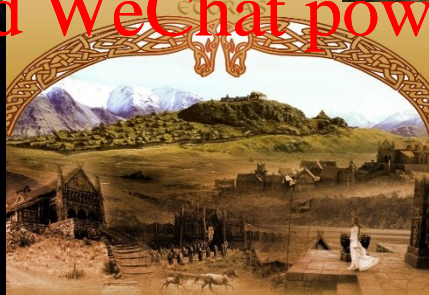
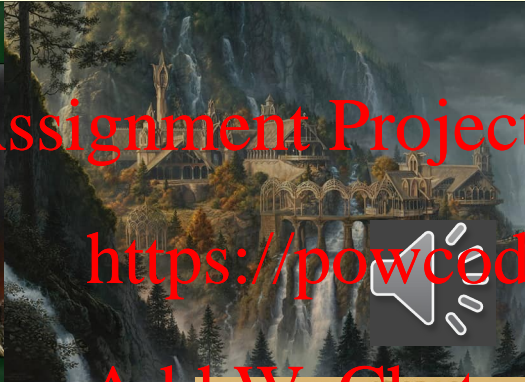
Thomas music means 1 minute left!



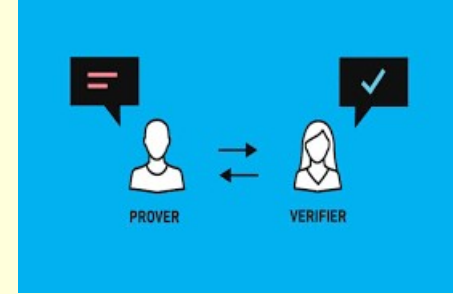
Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



3-colouring example



Secret: 3-colouring of a given graph G

Action:

- Peggy shows Victor the graph G
- Victor randomly chooses two adjacent nodes
- Peggy shows Victor the colouring of the two nodes
- Successful if the colour of both nodes is different



(shows graph G)

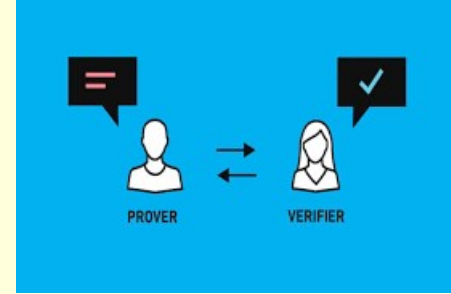


"Colours for these two nodes?" (chooses two adjacent nodes)

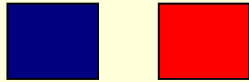


From: David Harel with Yishai Feldman, "Algorithmics: The Spirit of Computing" (3rd edition), Springer, 2012.

3-colouring example



"What are the colours of these two nodes?"



Assignment Project Exam Help
"What are the colours of these two nodes?"



<https://powcoder.com>



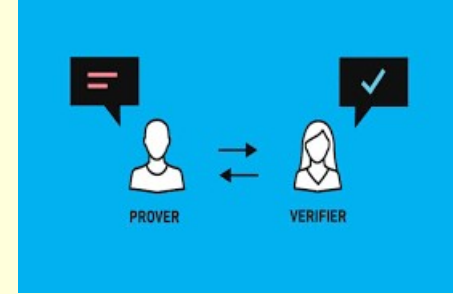
Add WeChat powcoder
"What are the colours of these two nodes?"



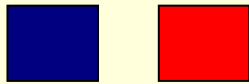
"What are the colours of these two nodes?"



3-colouring example



"What are the colours of these two nodes?"



Assignment Project Exam Help
"What are the colours of these two nodes?"



<https://powcoder.com>

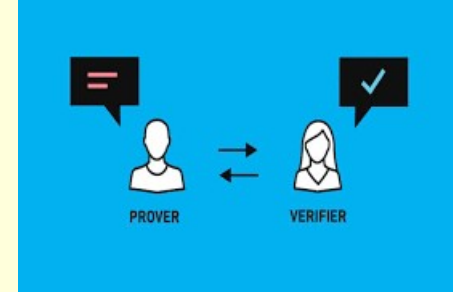
Add WeChat powcoder
"What are the colours of these two nodes?"



"Gotcha!"

"Oops!"

3-colouring example



- Victor randomly chooses an edge from the graph
- Peggy only shows colouring for these two nodes

Assignment Project Exam Help

Process continues until either the claim is disproved or the Victor gives up

<https://powcoder.com>

If the graph has n edges:

Add WeChat powcoder

Probability of passing 1 test falsely is $(n-1)/n$

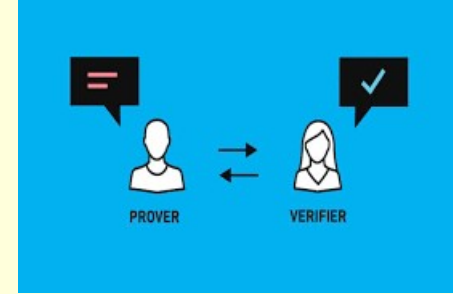
Probability of passing 2 tests falsely is $[(n-1)/n]^2$

Probability of passing 3 tests falsely is $[(n-1)/n]^3$

...

Probability of passing k tests falsely is $[(n-1)/n]^k$

3-colouring example



$N = 100$

$N = 200$

Trials	Probability of error
10	90.44%
20	81.79%
30	73.97%
40	66.90%
50	60.50%
60	54.72%
70	49.48%
80	44.75%
90	40.47%
100	36.60%

Trials	Probability of error
10	95.11%
20	90.46%
30	86.04%
40	81.83%
50	77.83%
60	74.03%
70	70.41%
80	66.96%
90	63.69%
100	60.58%

Computing Theory

Week 11

Questions?



Questions?



Assignment Project Exam Help

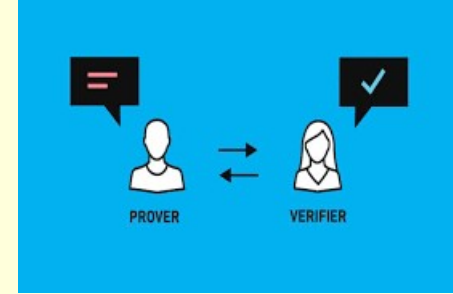
<https://powcoder.com>

Add WeChat powcoder

Questions?



3-colouring example



Issues

- Not very fast to an arbitrary probability
- How does Victor know Peggy is not just choosing randomly?

Assignment Project Exam Help

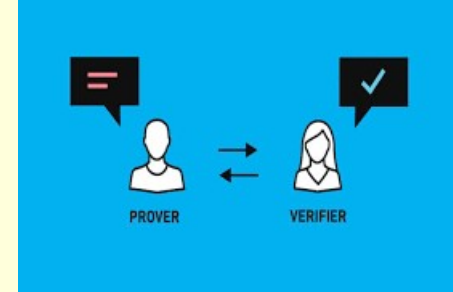
<https://powcoder.com>

Hamiltonian Cycle version

Add WeChat powcoder

- Similar use of 'guess and check' property of NP problems
- Requires cryptographic commitment from Peggy to the graph
- Victor can then check the cycle is really from the graph

Hamiltonian cycle version

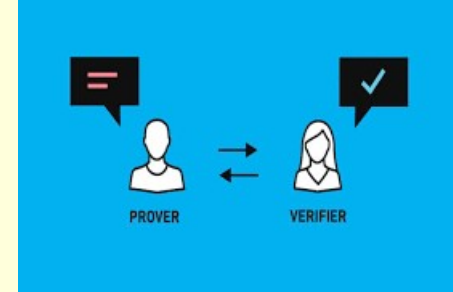


Secret: A Hamiltonian cycle of a given graph G

Action:

- Peggy creates an isomorphic copy of H (fast time) of G
- Peggy commits to H
- Victor randomly chooses to see either:
 1. The isomorphism between H and G
 2. The Hamiltonian cycle in H
- Peggy then shows Victor as below
 1. The mapping between H and G
 2. The Hamiltonian cycle in H
- Victor then verifies
 1. H and G are isomorphic
 2. The cycle is really made from edges in H
- Successful if **Victor is satisfied with the verification**

Hamiltonian cycle version



- Victor randomly chooses between the two options
- Peggy can easily generate isomorphic copies of G
- Peggy can easily generate the cycle in H from the cycle in G
- Victor never finds out both H and the Hamiltonian cycle in H
- Victor needs both to work out the Hamiltonian cycle in G
- The randomness of Victor's choice means that Peggy can't cheat by predicting requests and generating random answers

Similar performance to Ali Baba's cave:

- Probability of passing 1 test falsely is $(1/2)$
- Probability of passing 2 tests falsely is $(1/2)^2$
- Probability of passing 3 tests falsely is $(1/2)^3$
- ...
- Probability of passing n tests falsely is $(1/2)^n$

When $n = 20$, this is 0.0000009536 (!!) (99.9999046% correct)

Questions?



Questions?



Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Questions?



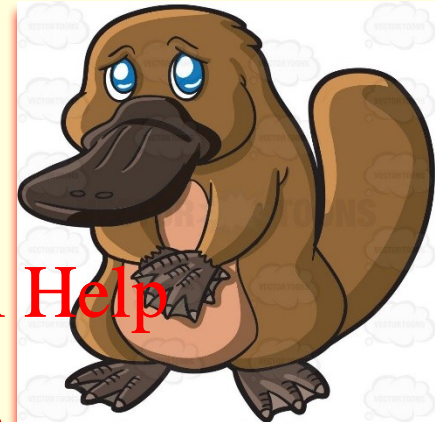
The Platypus Game

Assignment Project Exam Help

<https://powcoder.com>



Add WeChat powcoder



The Platypus Game

Assignment 2

Adding 10 machines

- Are they legal?
- Are they different from the existing 2,500?



extra.pl:

<https://powcoder.com>
extra(1, [t(y,k,g,k,gg),t(g,k,g,w,gg),t(y,e,y,w,wa),t(g,e,g,p,wa),t(y,w,y,w,gg),t(g,w,g,e,wa),t(y,p,y,k,wa)]).
extra(2, [t(y,k,y,k,gg),t(g,k,y,e,gg),t(y,e,y,p,wa),t(g,e,y,p,gg),t(y,w,y,p,wa),t(g,w,y,w,gg),t(y,p,g,e,wa)]).
extra(3, [t(y,k,y,k,wa),t(g,k,y,p,gg),t(y,e,g,p,wa),t(g,e,g,w,gg),t(y,w,g,p,wa),t(g,w,g,e,gg),t(y,p,y,w,gg)]).
extra(4, [t(y,k,g,e,wa),t(g,k,g,k,gg),t(y,e,y,k,gg),t(g,e,g,p,wa),t(y,w,y,p,wa),t(g,w,y,p,wa),t(y,p,g,e,wa)]).
extra(5, [t(y,k,g,k,wa),t(g,k,y,k,wa),t(y,e,y,p,wa),t(g,e,y,p,wa),t(y,w,g,e,gg),t(g,w,y,k,gg),t(y,p,y,e,wa)]).
extra(6, [t(y,k,y,e,wa),t(g,k,g,p,gg),t(y,e,g,w,wa),t(g,e,y,k,gg),t(y,w,y,w,gg),t(g,w,y,p,wa),t(y,p,g,e,gg)]).
extra(7, [t(y,k,g,e,gg),t(g,k,g,w,gg),t(y,e,y,w,wa),t(g,e,g,e,wa),t(y,w,g,e,gg),t(g,w,y,w,gg),t(y,p,y,p,gg)]).
extra(8, [t(y,k,y,k,wa),t(g,k,y,w,gg),t(y,e,g,w,wa),t(g,e,y,k,wa),t(y,w,g,w,gg),t(g,w,y,k,gg),t(y,p,y,e,gg)]).
extra(9, [t(y,k,g,w,wa),t(g,k,g,e,wa),t(y,e,g,w,wa),t(g,e,g,w,wa),t(y,w,g,k,wa),t(g,w,g,w,gg),t(y,p,g,e,gg)]).
extra(10, [t(y,k,g,w,gg),t(g,k,y,w,wa),t(y,e,g,p,gg),t(g,e,y,w,gg),t(y,w,y,p,wa),t(g,w,g,k,wa),t(y,p,y,e,gg)]).

The Platypus Game



Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

consult platypus7.pl

consult 2500 machines

consult new machines

run test

Computing Theory

SWI-Prolog (AMD64, Multi-threaded, version 8.2.1)

File Edit Settings Run Debug Help

Welcome to SWI-Prolog (threaded, 64 bits, version 8.2.1)

SWI-Prolog comes with ABSOLUTELY NO WARRANTY. This is free software.

Please run ?- license. for legal details.

For online help and background, visit <https://www.swi-prolog.org>

For built-in help, use ?- help(Topic). or ?- apropos(Word).

?- consult('C:/platypus/Code/Publish/platypus7.pl').

true.

?- consult('C:/platypus/Code/Publish/machines3.pl').

true.

?- consult('C:/platypus/Code/Publish/extra.pl').

true.

?- check_new.

All machines legal

The following machines are not new:

[t(y,k,g,k,wa),t(g,k,y,k,wa),t(y,e,y,p,wa),t(g,e,y,p,wa),t(y,w,g,e,gg),t(g,w,y,k,gg),t(y,p,y,e,wa)].

true.

?- |

Questions?



Questions?



Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Questions?



That's it!



I am out of here!

Assignment Project Exam Help

<https://powcoder.com>



Add WeChat powcoder



Break time! (We resume when all the pictures are gone! This will take 3 minutes!)



Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

