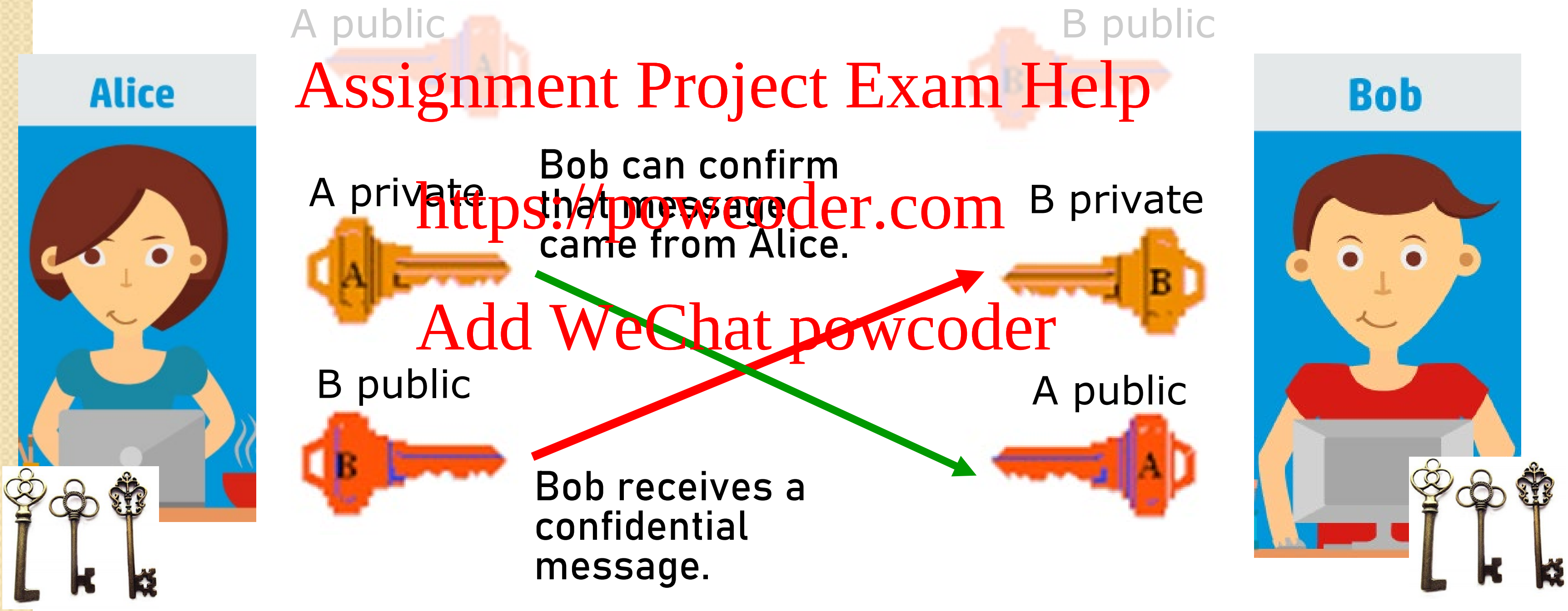


A public

B public

A private

Bob can confirm that message came from Alice.

B private

B public

A public

Bob receives a confidential message.

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

AES vs RSA vs DH

	AES	DH	RSA
symmetric/ asymmetric	symmetric	asymmetric	asymmetric
uses	**encrypt data** (symmetric key must be exchanged)	**generate symmetric key**	• encrypt data (slow) • **exchange symmetric key** (public keys must be known/exchanged) • **prove sender's authenticity** (public keys must be known/exchanged)

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

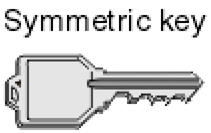
RSA Applications (cont.)

Challenges of confidential exchange of messages

Assignment Project Exam Help

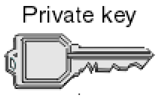
a) using symmetric encryption only: exchange of keys is a problem!

https://powcoder.com



Add WeChat powcoder

b) using asymmetric encryption only: algorithm is too slow!



Can we somehow combine the two?!

RSA Applications

- **Application of RSA Cryptography**
  - **protect. of data confidentiality & user/message authenticity**
  - other possible more common uses:

Assignment Project Exam Help

a) **digital envelopes** = fast exchange of confidential messages (secret message & secret key sent at once)

https://powcoder.com

Add WeChat powcoder

b) **digital signature** =

= **message integrity** + **message authentication**, where

message integrity – guarantees that the message has not been changed

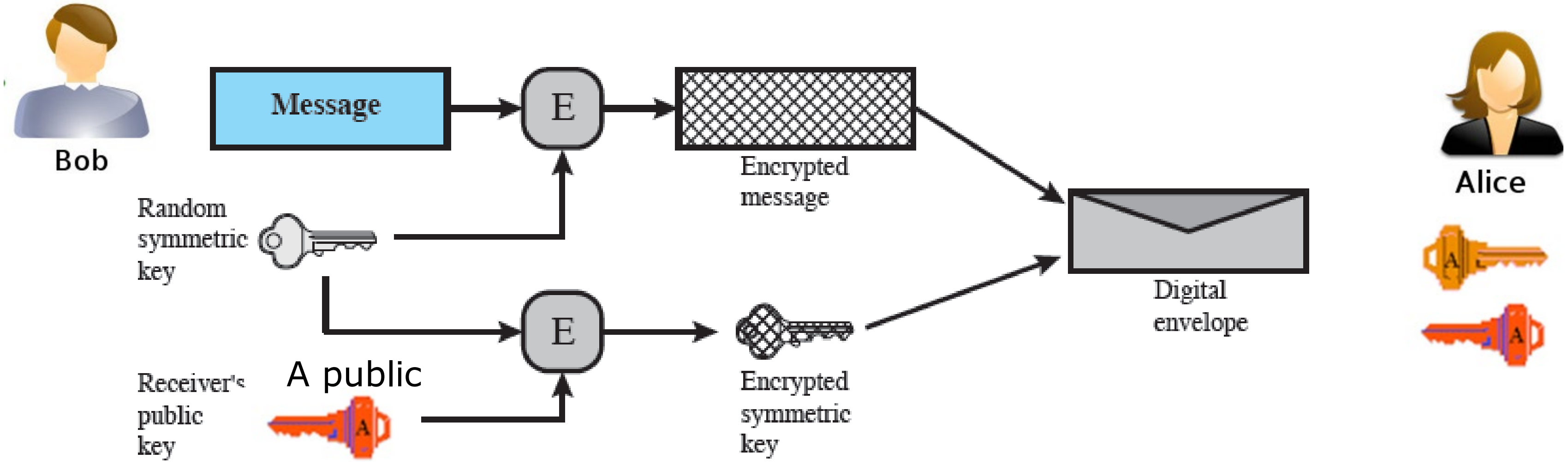
message authentication – authenticates the sender of the message

RSA Applications (cont.)

- **Digital Envelope** – use of asymmetric encryption for fast exchange of confidential messages

1) generate random symmetric key $K_{symmetric}$
2) encrypt message using $K_{symmetric}$ - digital letter
3) encrypt $K_{symmetric}$ using receiver’s public key K^+ - protective digital envelope
4) send the two together !!!

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder



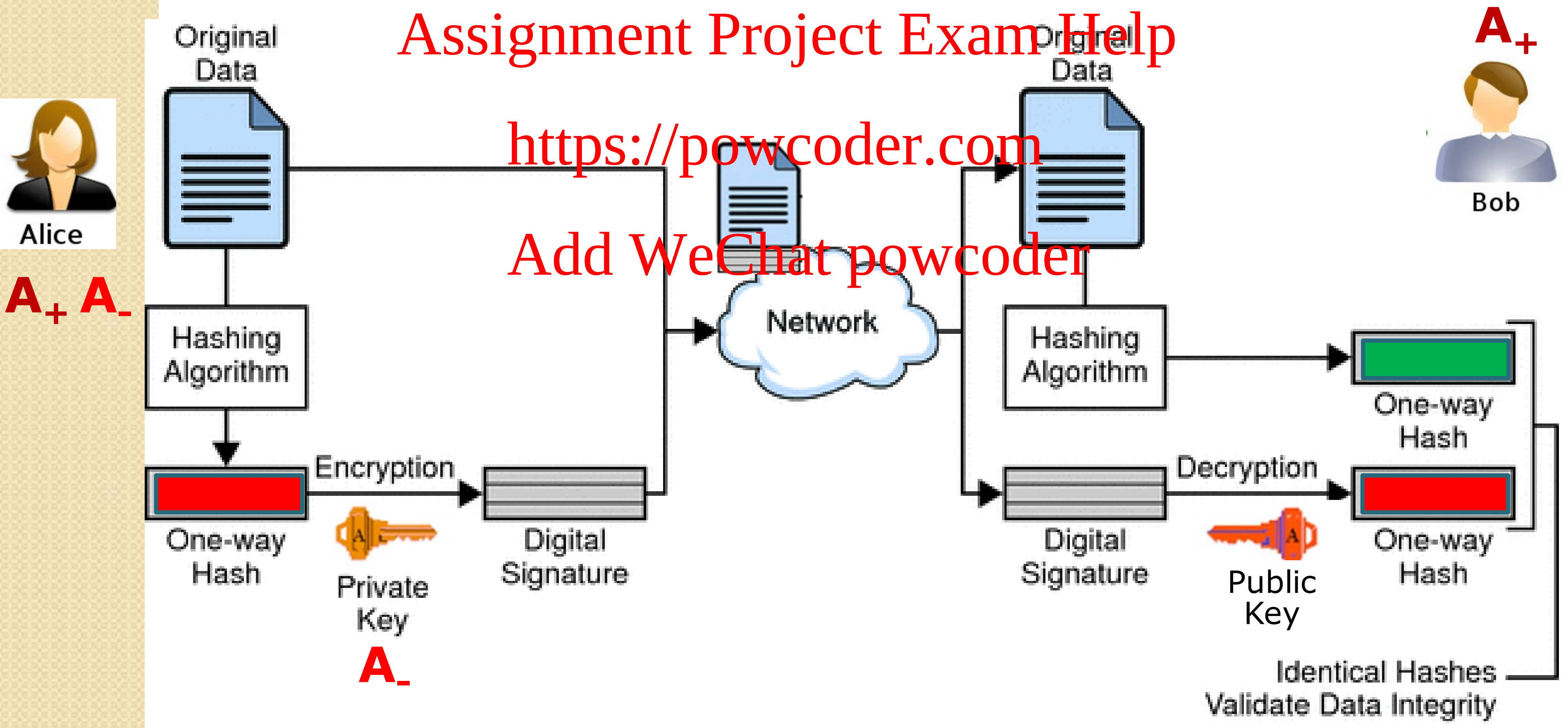
RSA Applications (cont.)

- **Digital Signature** - use of asymmetric encryption to protect message integrity + sender authenticity

Assignment Project Exam Help

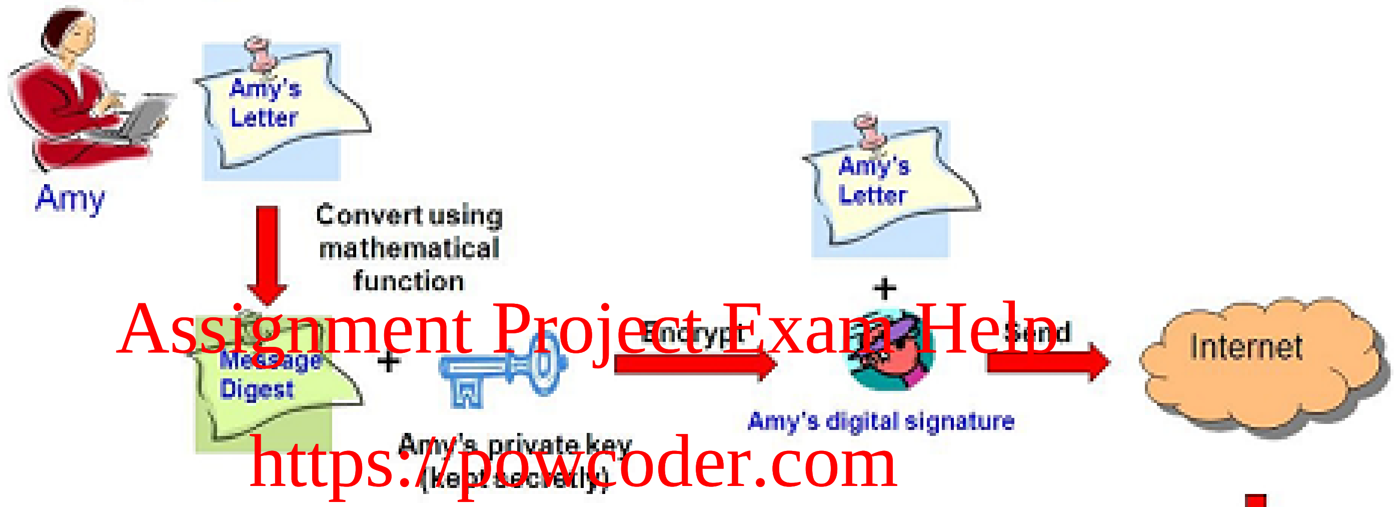
https://powcoder.com

Add WeChat powcoder

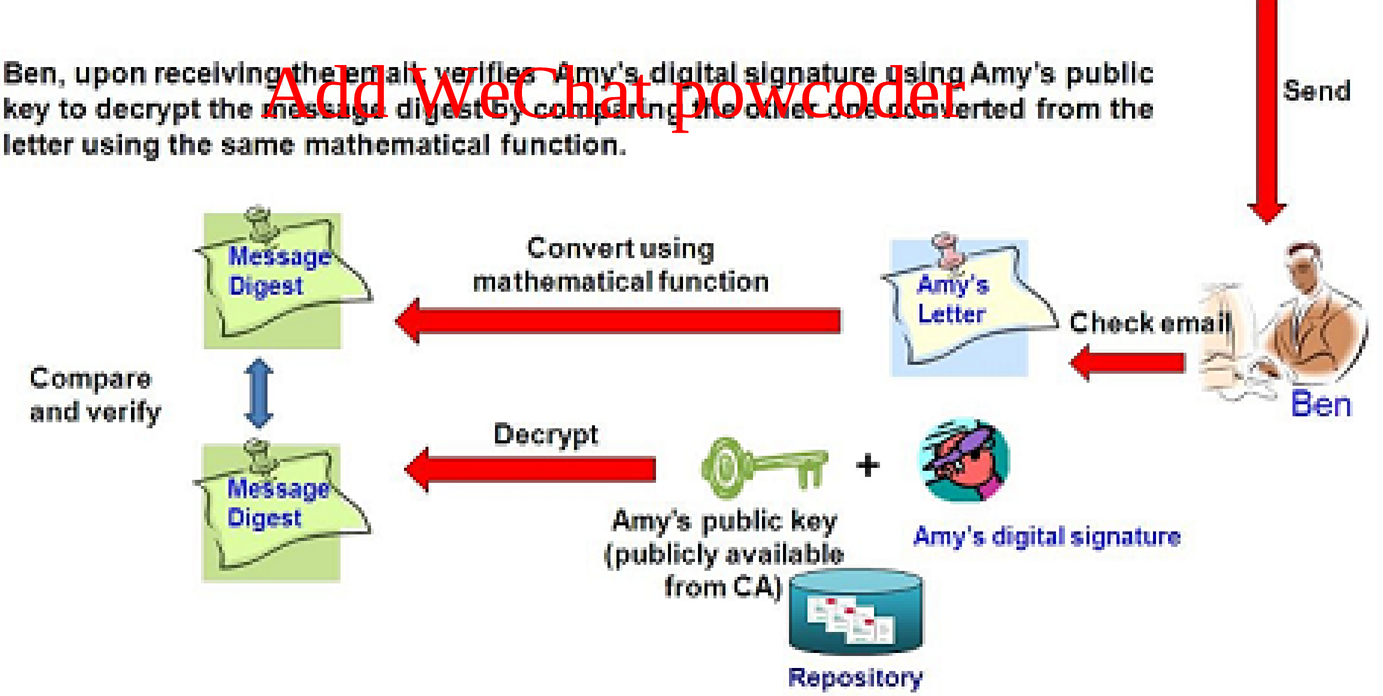


Digital Signature

1. Amy converts her letter into a message digest by using a mathematical function. She then creates her digital signature by encrypting the message digest using her private key. Her letter, together with her digital signature are sent to Ben via email.



2. Ben, upon receiving the email, verifies Amy's digital signature using Amy's public key to decrypt the message digest by comparing the other one converted from the letter using the same mathematical function.



Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

RSA Application (cont.)

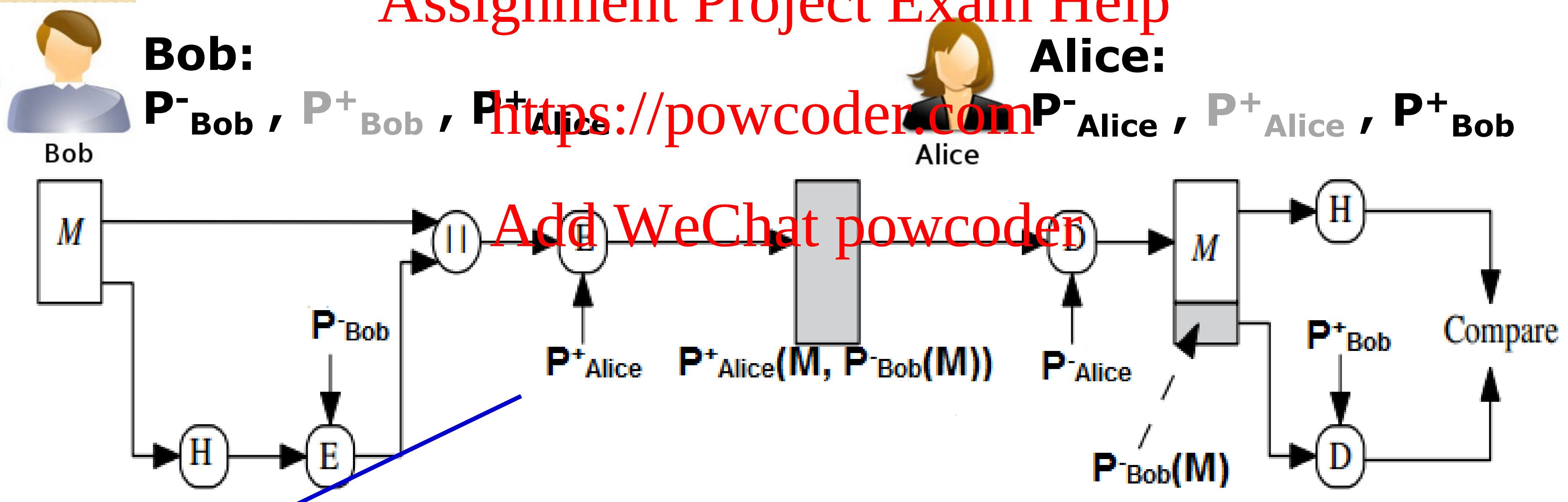
Example: Public encryption for all three – message integrity, authentication and confidentiality

(digital signatures + confidentiality)

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder



Bob: P^-_{Bob} , P^+_{Bob} , P^+_{Alice}

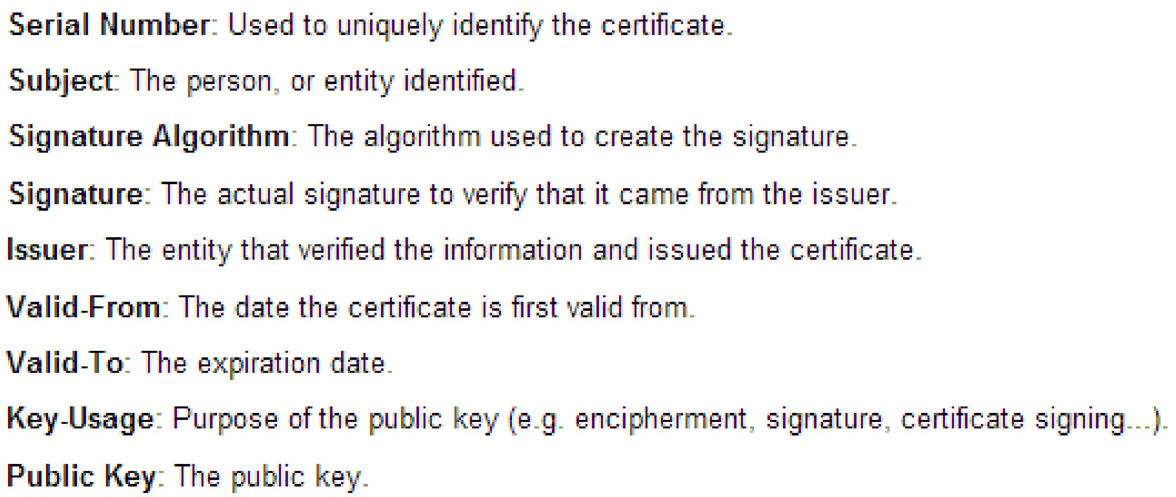
Alice: P^-_{Alice} , P^+_{Alice} , P^+_{Bob}

What is the (only) drawback here?!

NOTE: this is theoretically OK, but practically very slow. A better solution would be for Bob to generate a symmetric key K, use K to encrypt the message & digest, and send K encrypted using Alice's public key …

Public-Key / Digital Certificates

- **Reliable Public-Key Distribution** – must involve a trusted third party
  - **Certificate Authority** – a trusted government agency or a for-profit institution that issues Digital Certificates
    - IdenTrust, DigiCert, GlobalSign, …
  - **Digital Certificate** – digital document that binds a public key to an identity (person or organization) and contains:



Serial Number: Used to uniquely identify the certificate.

Subject: The person, or entity identified.

Signature Algorithm: The algorithm used to create the signature.

Signature: The actual signature to verify that it came from the issuer.

Issuer: The entity that verified the information and issued the certificate.

Valid-From: The date the certificate is first valid from.

Valid-To: The expiration date.

Key-Usage: Purpose of the public key (e.g. encipherment, signature, certificate signing...).

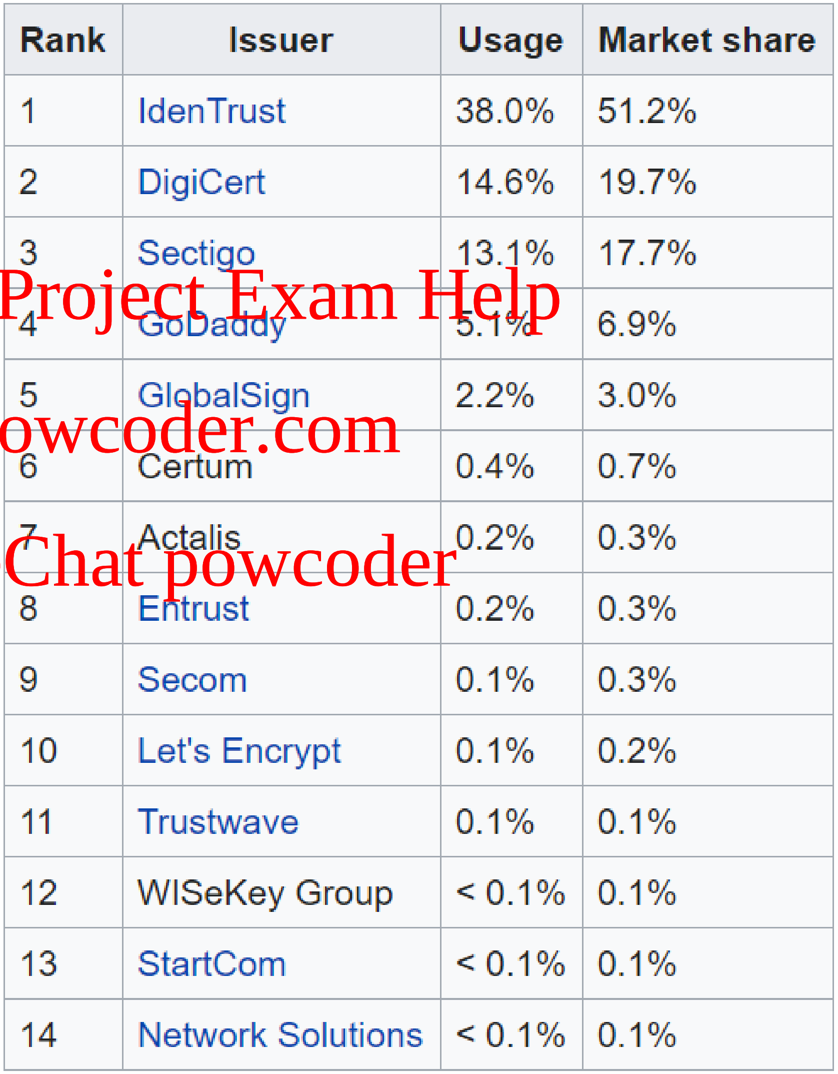
Public Key: The public key.

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Public-Key / Digital Certificates (cont.)

Example:

CA Prevalence



Rank	Issuer	Usage	Market share
1	IdenTrust	38.0%	51.2%
2	DigiCert	14.6%	19.7%
3	Sectigo	13.1%	17.7%
4	GoDaddy	5.1%	6.9%
5	GlobalSign	2.2%	3.0%
6	Certum	0.4%	0.7%
7	Actalis	0.2%	0.3%
8	Entrust	0.2%	0.3%
9	Secom	0.1%	0.3%
10	Let's Encrypt	0.1%	0.2%
11	Trustwave	0.1%	0.1%
12	WISeKey Group	< 0.1%	0.1%
13	StartCom	< 0.1%	0.1%
14	Network Solutions	< 0.1%	0.1%

Assignment Project Exam Help

https://powcoder.com

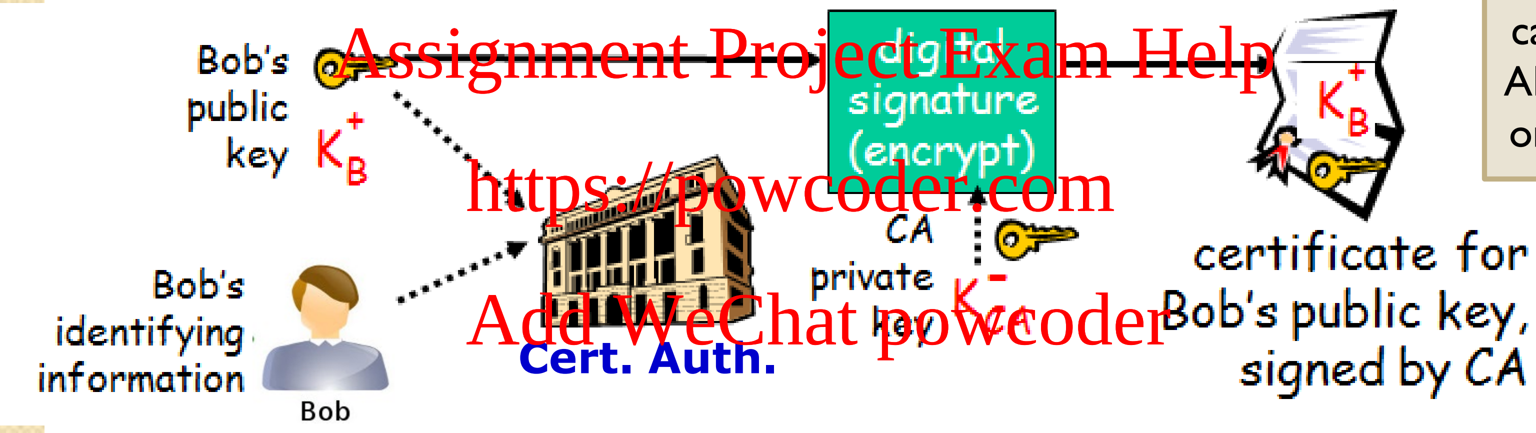
Add WeChat powcoder

https://en.wikipedia.org/wiki/Certificate_authority

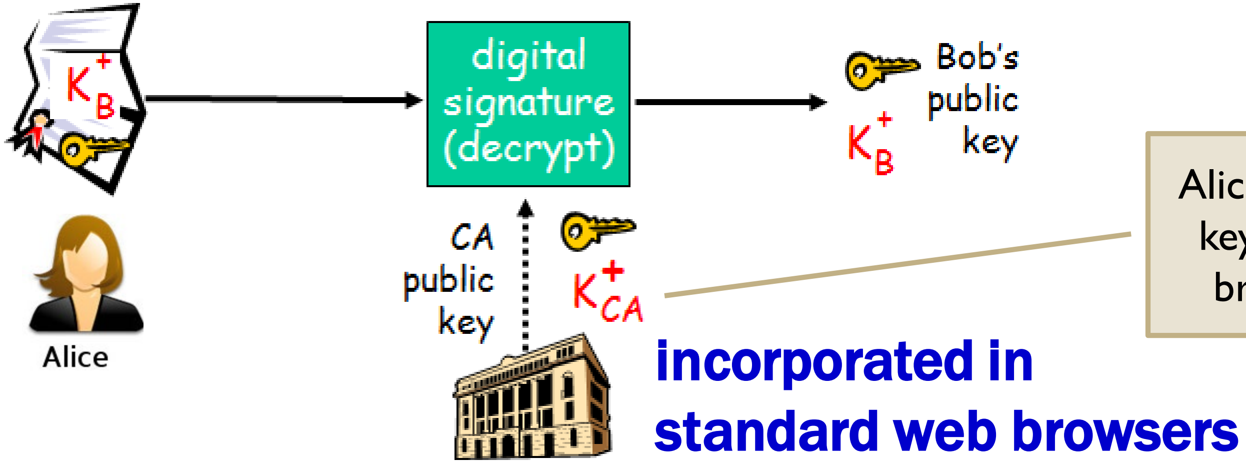
Public-Key / Digital Certificates (cont.)

Example: Creation of public-key certificate: creation and use

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder


Bob's public key
K_B^+
digital signature (encrypt)
K_B^+
CA private key
K_{CA}^-
certificate for Bob's public key, signed by CA
Bob's identifying information
Bob
Cert. Auth.

Bob gets this certificate and can send it to Alice or install on his server!

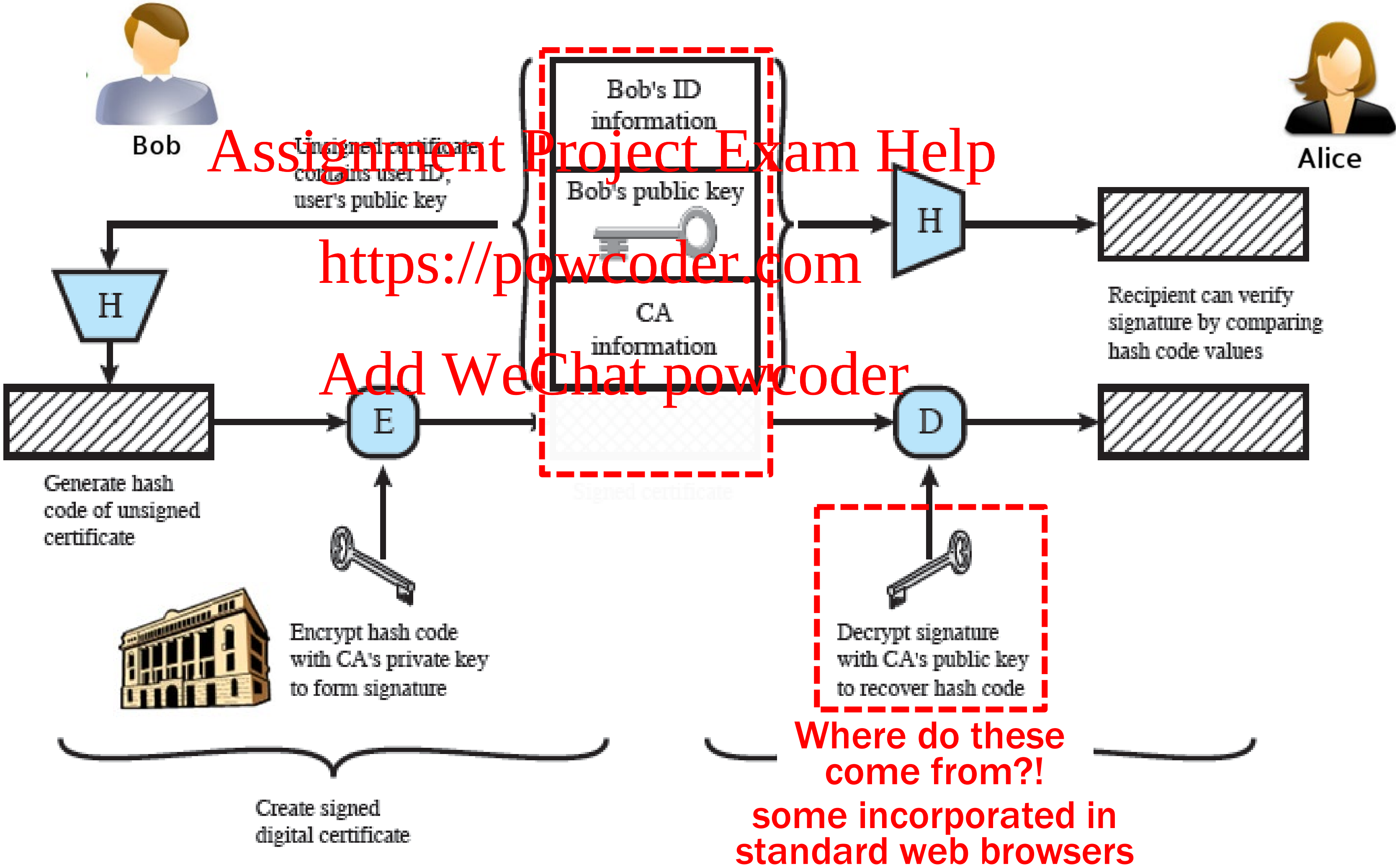


incorporated in standard web browsers

Alice has this key on her browser!

Public-Key / Digital Certificates (cont.)

Example: Creation & verification of a digital certificate



Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Where do these come from?!

some incorporated in standard web browsers

Encoding vs. Encryption vs. Hashing

Message Encoding vs. Encryption vs. Hashing

- all three transform message into another 'format'
- encoding and encryption are reversible, hashing is not!

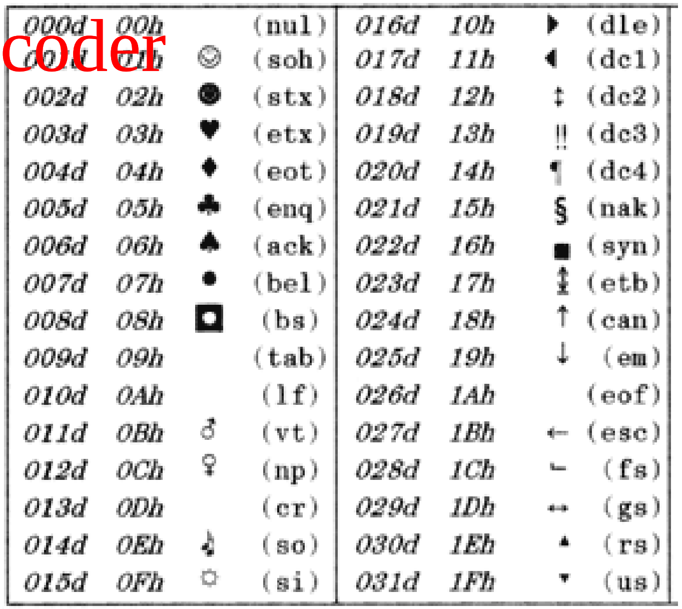
Assignment Project Exam Help

1) **message encoding** – transforms data to another format so that it can be properly/safely consumed by a different type of system

https://powcoder.com

Add WeChat powcoder

- does not aim to keep information secret
- does not require a key
- encoding scheme is publicly available and relatively simple/fast to perform



000d	00h		(nul)	016d	10h	►	(dle)
001d	01h	☺	(soh)	017d	11h	◄	(dc1)
002d	02h	☻	(stx)	018d	12h	↕	(dc2)
003d	03h	♥	(etx)	019d	13h	‼	(dc3)
004d	04h	♦	(eot)	020d	14h	¶	(dc4)
005d	05h	♣	(enq)	021d	15h	§	(nak)
006d	06h	♠	(ack)	022d	16h	▬	(syn)
007d	07h	•	(bel)	023d	17h	↨	(etb)
008d	08h	◘	(bs)	024d	18h	↑	(can)
009d	09h		(tab)	025d	19h	↓	(em)
010d	0Ah		(lf)	026d	1Ah		(eof)
011d	0Bh	♂	(vt)	027d	1Bh	←	(esc)
012d	0Ch	♀	(np)	028d	1Ch	∟	(fs)
013d	0Dh		(cr)	029d	1Dh	↔	(gs)
014d	0Eh	♫	(so)	030d	1Eh	▲	(rs)
015d	0Fh	☼	(si)	031d	1Fh	▼	(us)

special characters on a web page

Encoding vs. Encryption vs. Hashing (cont.)

Message Encoding vs. Encryption vs. Hashing (cont.)

2) message encryption – transforms data to another format that cannot be easily consumed by anybody but the intended recipient(s)

Assignment Project Exam Help

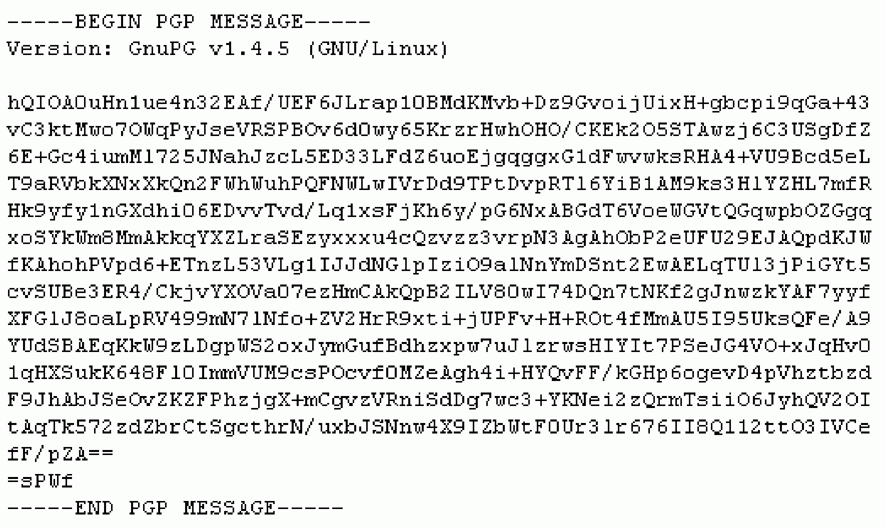
- aims to keep information secret

https://powcoder.com

- requires a key

Add WeChat powcoder

- encryption scheme is publicly available but quite complex to perform/break



```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.5 (GNU/Linux)

hQIOA0uHn1ue4n32EAf/UEF6JLrap1OBMdKMvb+Dz9GvoijUixH+gbcpi9qGa+43
vC3ktMwo7OWqPyJseVRSPBOv6d0wy65KrzrHwhOHO/CKEk2O5STAwzj6C3USgDfZ
6E+Gc4iumMl725JNahJzcL5ED33LFdZ6uoEjgqggxG1dFwvwksRHA4+VU9Bcd5eL
T9aRVbkXNxXkQn2FWhWuhPQFNWLwIVrDd9TPtDvpRTl6YiB1AM9ks3HlYZHL7mfR
Hk9yfy1nGXdhi06EDvvTvd/Lq1xsFjKh6y/pG6NxABGdT6VoeWGVtQGqwpbOZGgq
xoSYkWm8MmAkkqYXZLraSEzyxxxu4cQzvzz3vrpN3AgAhObP2eUFU29EJAQpdKJW
fKAhohPVpd6+ETnzL53VLg1IJJdNGlpIziO9alNnYmDSnt2EwAELqTUl3jPiGYt5
cvSUBe3ER4/CkjvYXOVa07ezHmCAkQpB2ILV8OwI74DQn7tNKf2gJnwzkYAF7yyf
XFGlJ8oaLpRV499mN7lNfo+ZV2HrR9xti+jUPFv+H+ROt4fMmAU5I95UksQFe/A9
YUdSBAEqKkW9zLDgpWS2oxJymGufBdhzxpw7uJlzrwsHIYIt7PSeJG4VO+xJqHvO
1qHXSukK648Fl0ImmVUM9csPOcvfOMZeAgh4i+HYQvFF/kGHp6ogevD4pVhztbzd
F9JhAbJSeOvZKZFPhzjgX+mCgvzVRniSdDg7wc3+YKNei2zQrmTsii06JyhQV2OI
tAqTk572zdZbrCtSgcthrN/uxbJSNnw4X9IZbWtFOUr3lr676II8Q112ttO3IVCe
fF/pZA==
=sPWf
-----END PGP MESSAGE-----
```

Encoding vs. Encryption vs. Hashing (cont.)

Message Encoding vs. Encryption vs. Hashing (cont.)

3) **message hashing** – used to **validate the integrity** of a given content by producing a fixed-length string with following attributes:

Assignment Project Exam Help

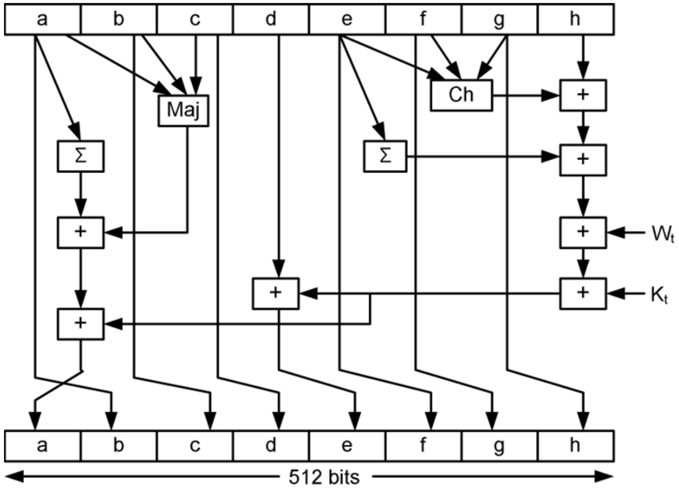
- does not require a key

https://powcoder.com

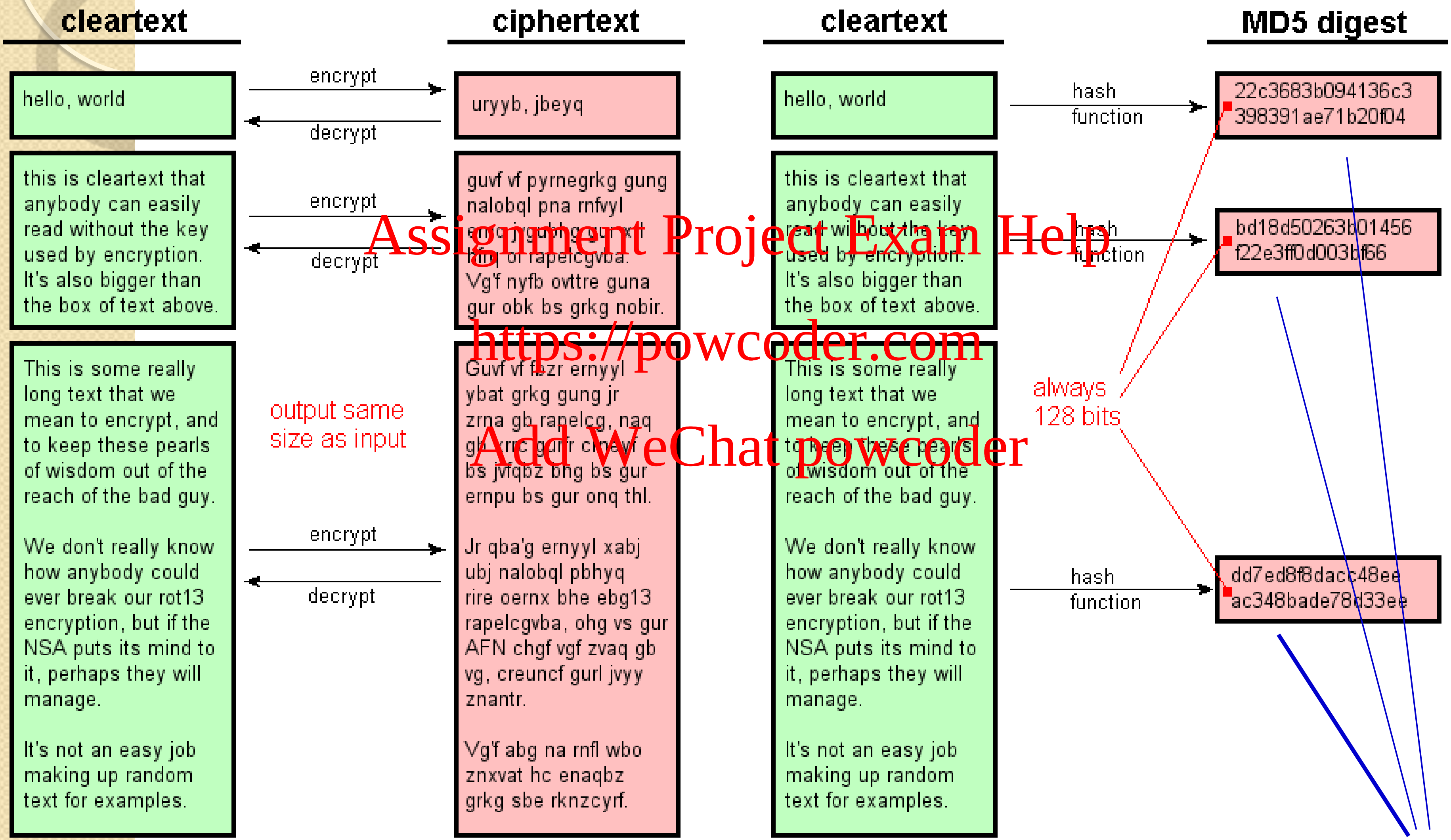
- hashing algorithms are publically available

Add WeChat powcoder

- the same input will always produce the same output
- any modification to the input should result in drastic change to the output



Encoding vs. Encryption vs. Hashing (cont.)



hello, world

uryyb, jbeyq

this is cleartext that anybody can easily read without the key used by encryption. It's also bigger than the box of text above.

guvf vf pyrnegrkg gung nalobql pna rnfvyl ernq jvgubhg gur xrl hfrq ol rapelcgvba. Vg'f nyfb ovttre guna gur obk bs grkg nobir.

This is some really long text that we mean to encrypt, and to keep these pearls of wisdom out of the reach of the bad guy.

We don't really know how anybody could ever break our rot13 encryption, but if the NSA puts its mind to it, perhaps they will manage.

It's not an easy job making up random text for examples.

Guvf vf fbzr ernyyl ybat grkg gung jr zrna gb rapelcg, naq gb xrrc gurfr crneyf bs jvfqbz bhg bs gur ernpu bs gur onq thl.

Jr qba'g ernyyl xabj ubj nalobql pbhyq rire oernx bhe ebg13 rapelcgvba, ohg vs gur AFN chgf vgf zvaq gb vg, creuncf gurl jvyy znantr.

Vg'f abg na rnfl wbo znxvat hc enaqbz grkg sbe rknzcyrf.

hello, world

this is cleartext that anybody can easily read without the key used by encryption. It's also bigger than the box of text above.

This is some really long text that we mean to encrypt, and to keep these pearls of wisdom out of the reach of the bad guy.

We don't really know how anybody could ever break our rot13 encryption, but if the NSA puts its mind to it, perhaps they will manage.

It's not an easy job making up random text for examples.

22c3683b094136c3 398391ae71b20f04

bd18d50263b01456 f22e3ff0d003bf66

dd7ed8f8dacc48ee ac348bade78d33ee

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

In case of hashing, the output 'size' is always constant / does not depend on the size of the input !!!

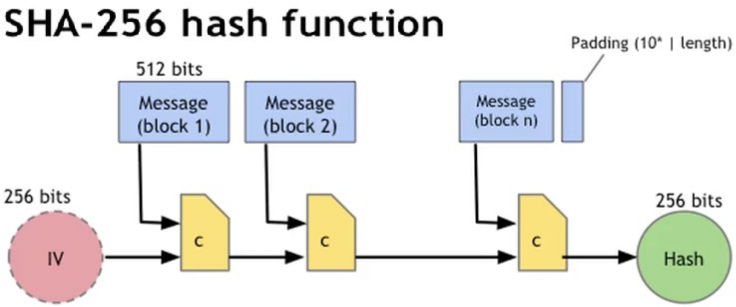
Hashing

- **Message Integrity** – accomplished through the use of <u>cryptographic hash functions</u>
  - hash function creates a <u>small</u> <u>fixed-size</u> digital 'summary' of the message that can be used as a <u>message fingerprint</u>, aka <u>hash</u> or <u>message digest</u>
  - typical hash size: 128, 160, 256, 512 bits
  - popular standards:

    (a) Message Digest 5 (MD5) – no longer secure

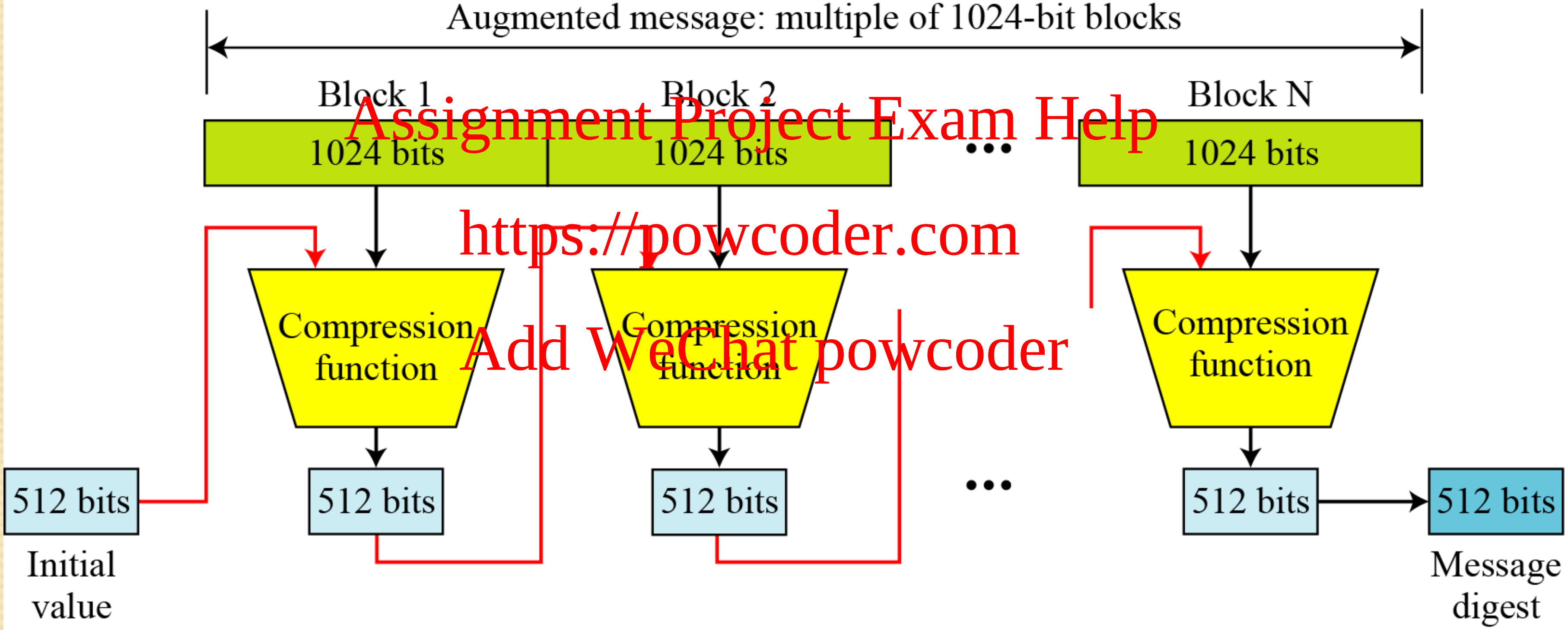
    (b) Secure Hash Algorithm (SHA-2: SHA 256 & SHA 512)

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

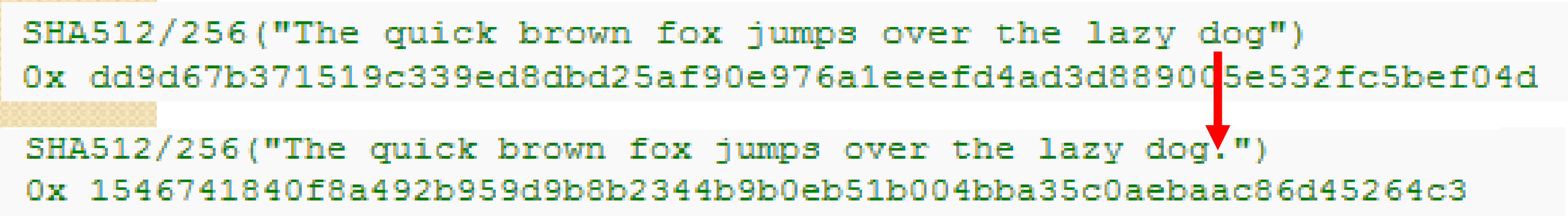


Hashing (cont.)

Example: Message digest creation with SHA-512



Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder



```
SHA512/256("The quick brown fox jumps over the lazy dog")
0x dd9d67b371519c339ed8dbd25af90e976a1eeefd4ad3d889005e532fc5bef04d

SHA512/256("The quick brown fox jumps over the lazy dog.")
0x 1546741840f8a492b959d9b8b2344b9b0eb51b004bba35c0aebaac86d45264c3
```

Hashing (cont.)

- **Hash Function Criteria** – to be eligible for a hash a function needs to meet 6 important criteria:
  - Hash function h can be applied to block of data of any size.
  - Hash function h produces a fixed-length output.
  - h(M) is relatively easy to compute for any given M, making both hardware and software implementation practical.
  - **Collision Resistance**.
  - **Preimage Resistance**.
  - **Second Preimage Resistance**.

Assignment Project Exam Help

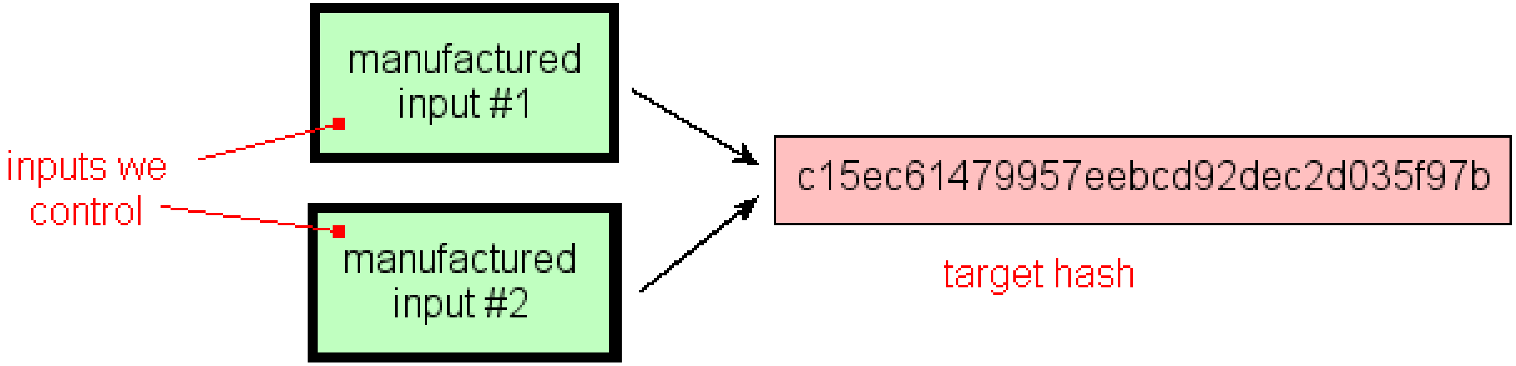
https://powcoder.com

Add WeChat powcoder

Hashing (cont.)

- Hash Function Criteria (cont.):
  - *collision: two messages create the same digest*
  - **Collision Resistance** or **Strong Collision Resistance**: must be *extremely difficult* to find **any two** M and M' such that h(M) = h(M')
  - if strong collision is possible => digital signatures become meaningless
  - *example/application: online password cracking*

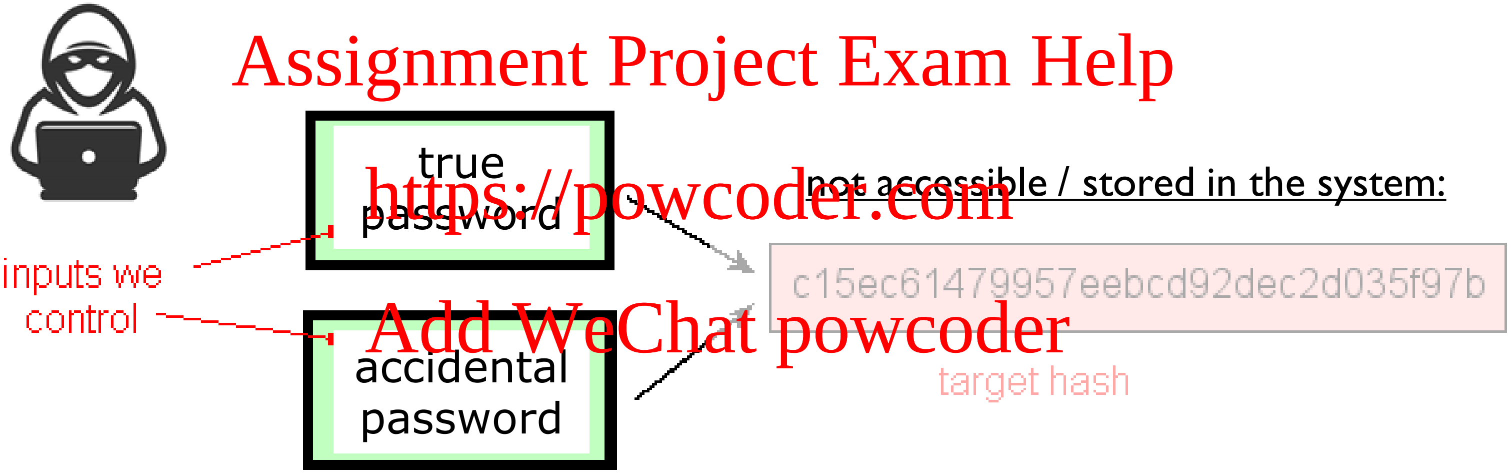
Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder



Hashing (cont.)

Example: Strong Collision Resistance example

(online password cracking)



Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

inputs we control

true password

accidental password

not accessible / stored in the system:

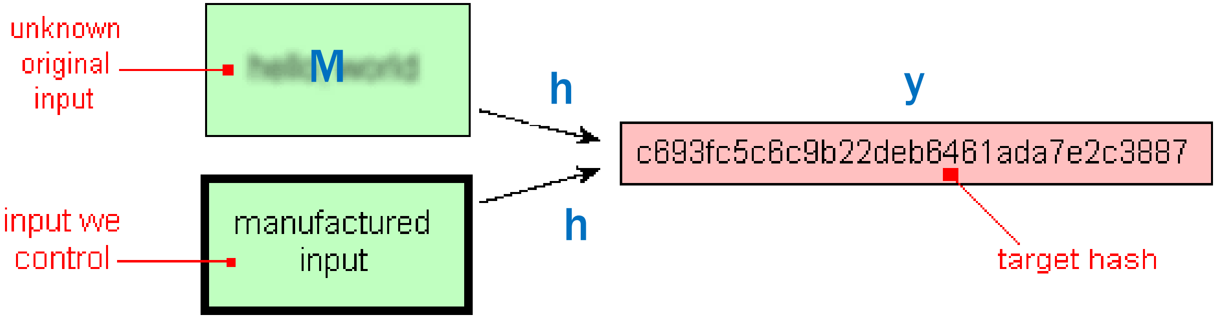
c15ec61479957eebcd92dec2d035f97b

target hash

Message Integrity (cont.)

- Hash Function Criteria (cont.):
  - **Preimage Resistance** or **One Wayness**: given a hash function h and y=h(M), it must be extremely difficult for Eve to find <u>any</u> message M’ such that y=h(M’)
  - we should <u>not</u> be able to work ‘backwards’ and (re)create the original message from a given hash
  - *example/application: off-line password cracking*

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder



http://www.unixwiz.net/techtips/iguide-crypto-hashes.html

Message Integrity (cont.)

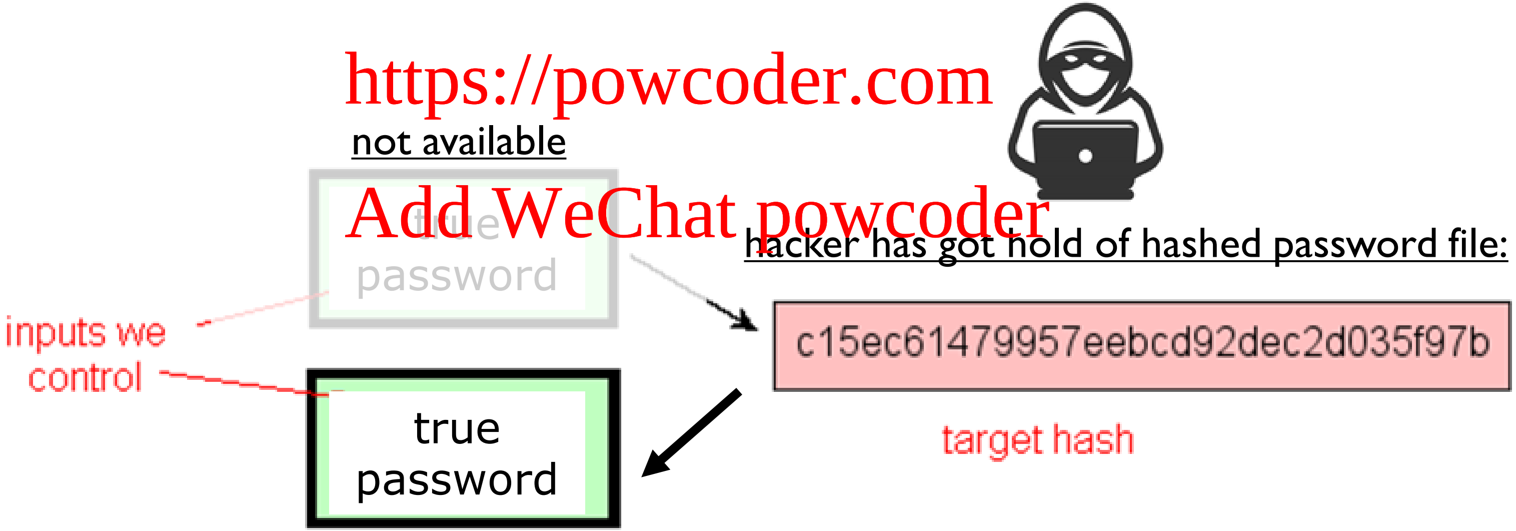
Example: **Preimage Resistance example**

(off-line password cracking)

Assignment Project Exam Help

https://powcoder.com

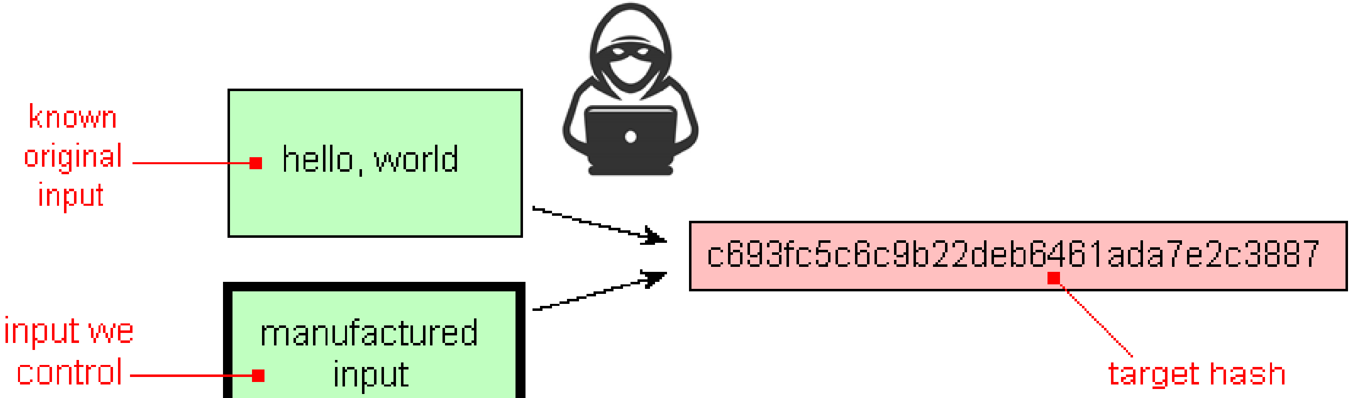
Add WeChat powcoder


not available
true password
hacker has got hold of hashed password file:
c15ec61479957eebcd92dec2d035f97b
target hash
inputs we control
true password

Hashing (cont.)

- Hash Function Criteria (cont.):
  - **Second Preimage Resistance** or **Weak Collision Resistance**: given M and its hash h(M) it should be extremely difficult for Eve to find a second/another message M' such that h(M)=h(M')
  - property intended to prevent an adversary from appending a falsified message to a given hash

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder



http://www.unixwiz.net/techtips/iguide-crypto-hashes.html

Hashing (cont.)

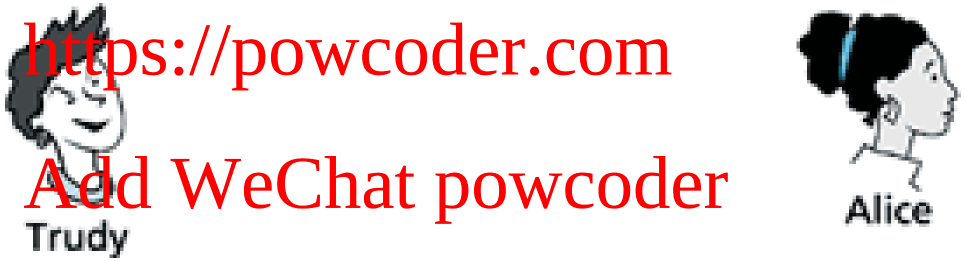
<u>Example</u>: Second Preimage Resistance example

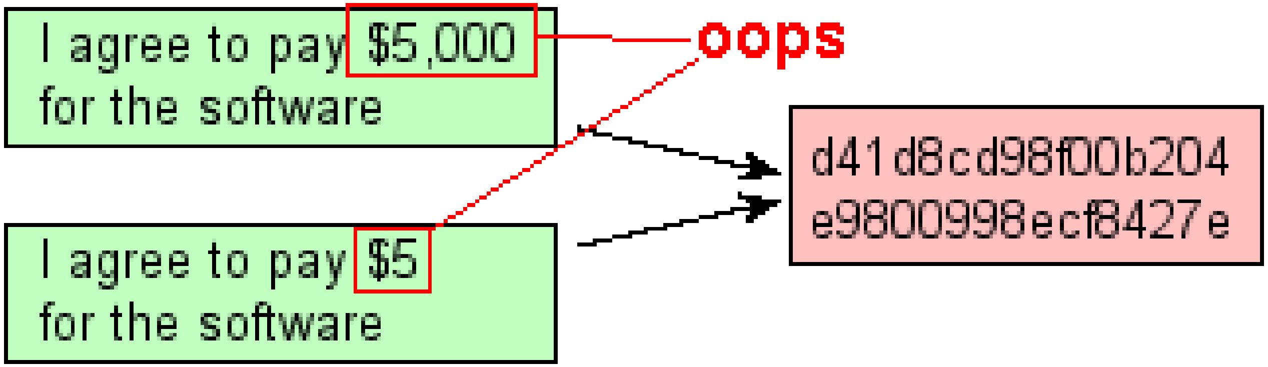
(alter the content of a ‘signed’ message)

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder





I agree to pay $5,000 for the software

I agree to pay $5 for the software

d41d8cd98f00b204 e9800998ecf8427e