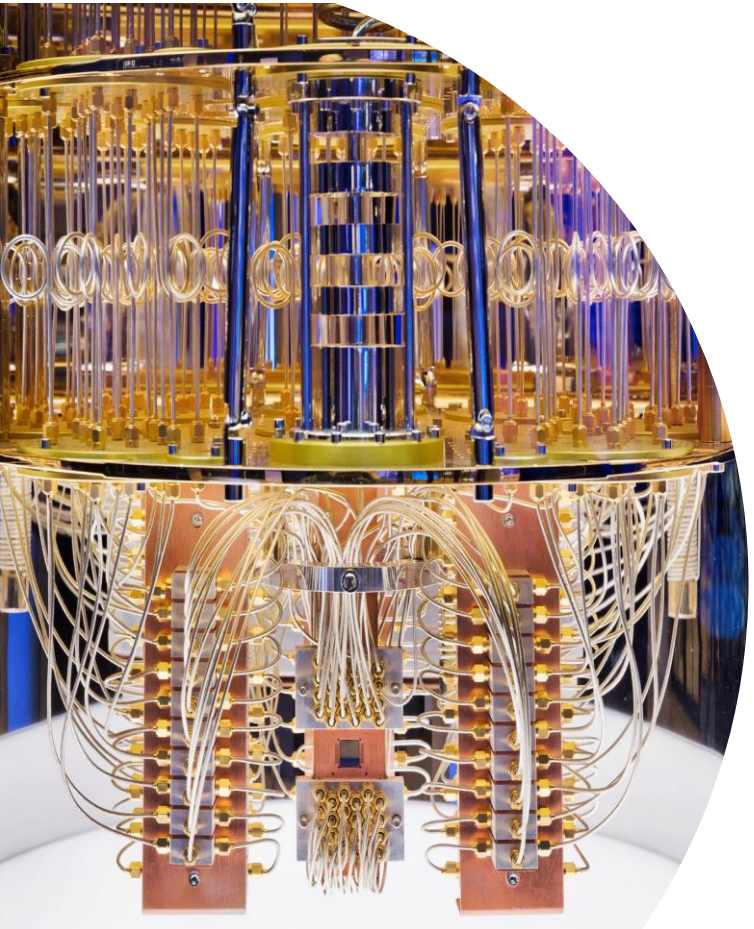
Post-quantum crypto: Countering future attacks that break today's messages

SNiC 2022

Kathrin Hövelmanns

November 30th, 2022

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY



How are these pictures related?

Brief history of communicating secrets

Scytale

Bodymod steganography
(Herodotus)

Caesar cipher

700 BC

440 BC

50 BC

Brief history of communicating secrets

Scytale

Bodymod steganography
(Herodotus)

Caesar cipher

‚Add 3‘ rule:

A	→	D
T		W
T		W
A		D
C		F
K		N

700 BC

440 BC

50 BC

Brief history of communicating secrets

Scytale

Bodymod steganography
(Herodotus)

Caesar cipher

Problem:

Techniques will never remain secret.

700 BC

440 BC

50 BC

Brief history of communicating secrets

Scytale

Bodymod steganography (Herodotus)

Caesar cipher

'It should not be a problem if [the system] falls into enemy hands.'

Kerckhoffs, 1883

700 BC

440 BC

50 BC

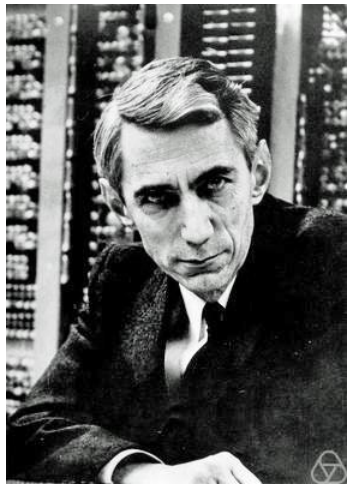
Brief history of communicating secrets

Scytale

Bodymod steganography
(Herodotus)

Caesar cipher

'The enemy knows the system.'



Shannon, 1949

700 BC

440 BC

50 BC

Brief history of communicating secrets

Scytale

Bodymod steganography
(Herodotus)

Caesar cipher

700 BC

440 BC

50 BC

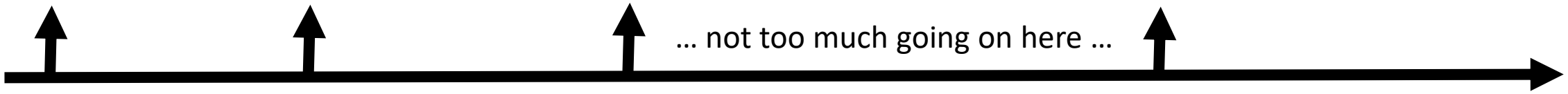
Brief history of communicating secrets

Scytale

Bodymod steganography
(Herodotus)

Caesar cipher

Vigenère



Brief history of communicating secrets

‚Caesar with codeword‘:

Codeword:
CRYPTO

A	A -> C	C
T	A -> R	K
T	A -> Y	R
A	A -> P	P
C	A -> T	V
K	A -> O	Y

Vigenère

… not too much going on here …

700 BC

440 BC

50 BC

1500 AD

Brief history of communicating secrets

‚Caesar with codeword‘:

Codeword:
CRYPTO

A	A -> C	C
T	A -> R	K
T	A -> Y	R
A	A -> P	P
C	A -> T	V
K	A -> O	Y

No codeword -> no secret

Vigenère

… not too much going on here …

700 BC

440 BC

50 BC

1500 AD

Brief history of communicating secrets

‚Caesar with codeword‘:

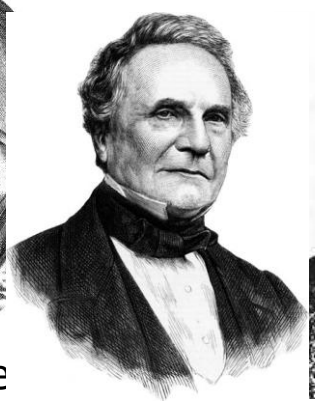
Codeword:
CRYPTO

A	A -> C	C
T	A -> R	K
T	A -> Y	R
A	A -> P	P
C	A -> T	V
K	A -> O	Y

No codeword -> no secret

Actually… Statistics!

Vigenère



Babbage
1854

Kasiski
1863

… not too much going on here …

700 BC

440 BC

50 BC

1500 AD

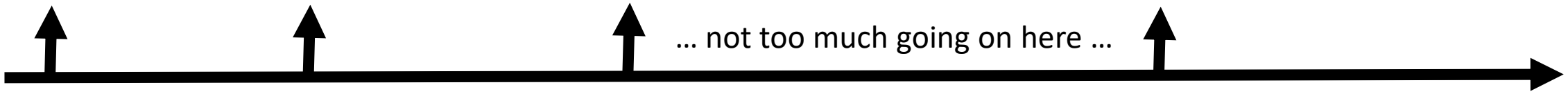
Brief history of communicating secrets

Scytale

Bodymod steganography
(Herodotus)

Caesar cipher

Vigenère



Brief history of communicating secrets

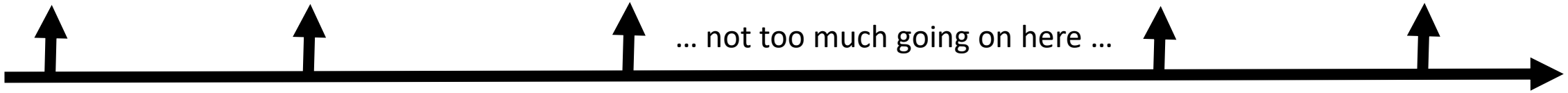
Scytale

Bodymod steganography (Herodotus)

Caesar cipher

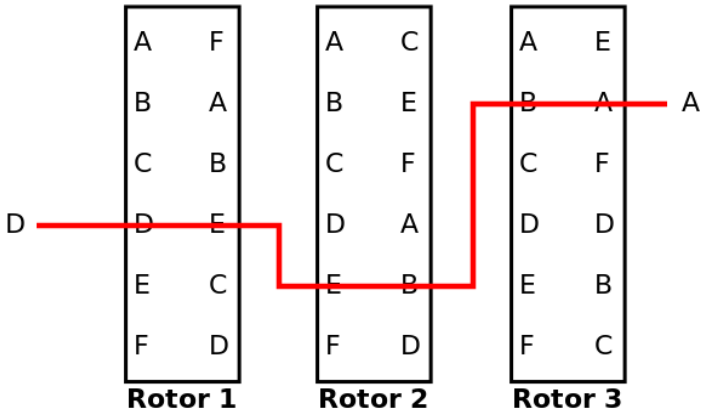
Vigenère

Enigma



Brief history of communicating secrets

Scrambling letters multiple times:



turning after each keystroke

Scyta

Vigenère

Enigma

… not too much going on here …

700 BC

440 BC

50 BC

1500 AD

1930 AD

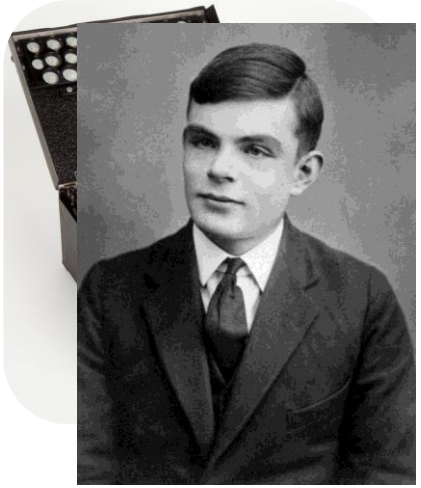
Brief history of communicating secrets

Scytale

Bodymod steganography (Herodotus)

Caesar cipher

Vigenère



Turing broke Enigma

… not too much going on here …

700 BC

440 BC

50 BC

1500 AD

1930 AD

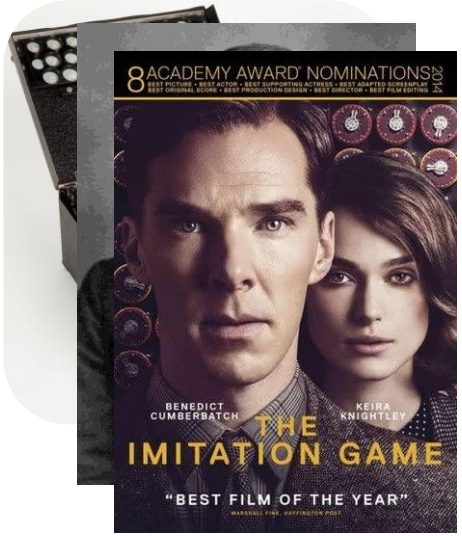
Brief history of communicating secrets

Scytale

Bodymod steganography (Herodotus)

Caesar cipher

Vigenère



and got movie famous

700 BC

440 BC

50 BC

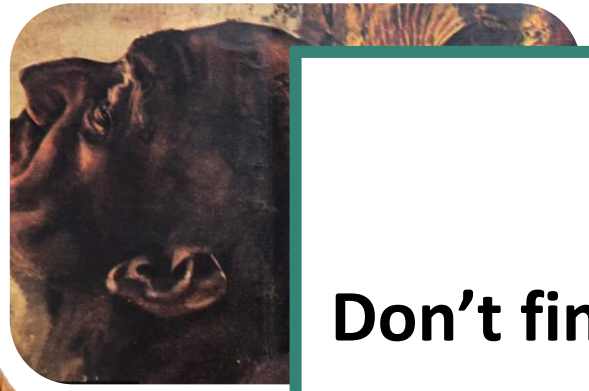
… not too much going on here …

1500 AD

1930 AD

Brief history of communicating secrets

Scytale



Bodymod st
(Hero

Problem 1:

Don’t find any attacks against your secret communication?

Doesn’t mean no one else does!

Caesar cipher

Vigenère

and got movie famous

… not too much going on here …

700 BC

440 BC

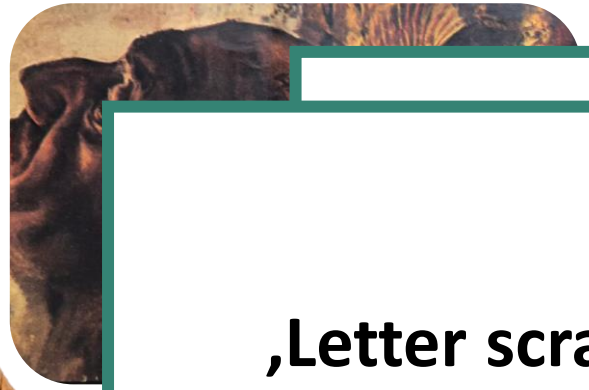
50 BC

1500 AD

1930 AD

Brief history of communicating secrets

Scytale



Bo

Problem 2:

‚Letter scrambling' needs a shared secret.

How to get it from A to B?

tion?

broke Vigenère cipher

famous

… not too much going on here …

700 BC

440 BC

50 BC

1500 AD

1930 AD

Brief history of communicating secrets

Enigma

Public-Key Crypto

Avoids pre-shared secrets!

1930

Late 1970s

Brief history of communicating secrets

Enigma

Public-Key Crypto

Merkle, Hellman, Diffie

Rivest, Shamir, Adleman

1930

Late 1970s

Brief history of communicating secrets

Enigma

Public-Key Crypto

Ellis, Cocks, Williamson

Merkle, Hellman, Diffie

Rivest, Shamir, Adleman

1930

1973

Late 1970s

Brief history of communicating secrets

Enigma

Public-Key Crypto

Ellis, Cocks, Williamson

(until 1997)

Merkle, Hellman, Diffie

Rivest, Shamir, Adleman

1930

1973

Late 1970s

Today, crypto is much more!

Why care?

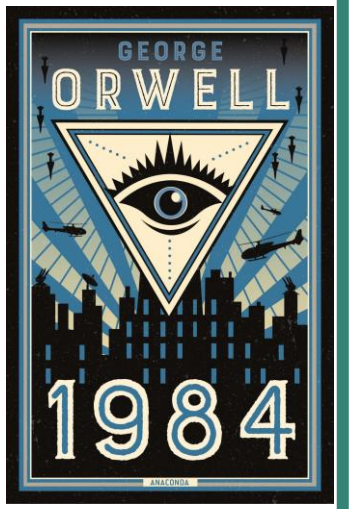
Why care?

Why care?

Miller attempts to rescue the Jeep after its brakes were remotely disabled, sending it into a ditch. ANDY GREENBERG/WIRED

Why care?

Got nothing to hide?



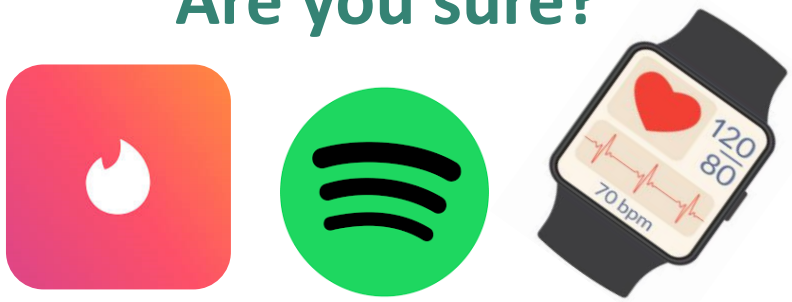
Why care?

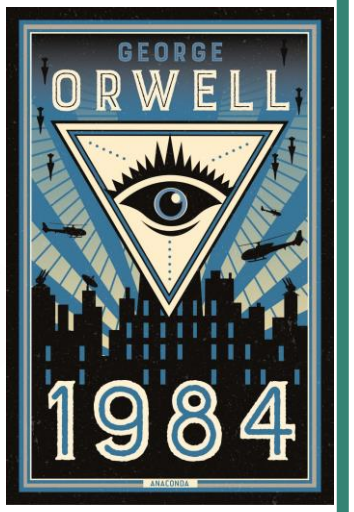

Got nothing to hide?
Are you sure?
120
80
70 bpm
GEORGE
ORWELL
1984

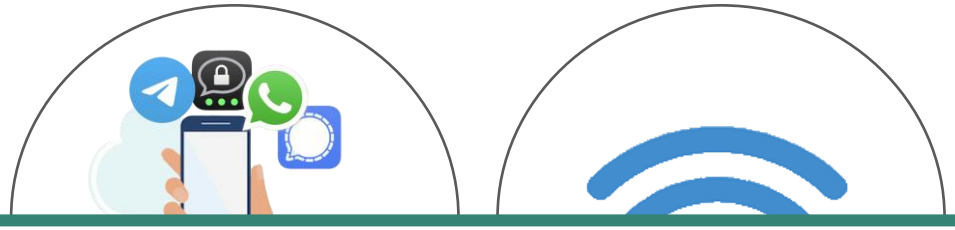
Why care?

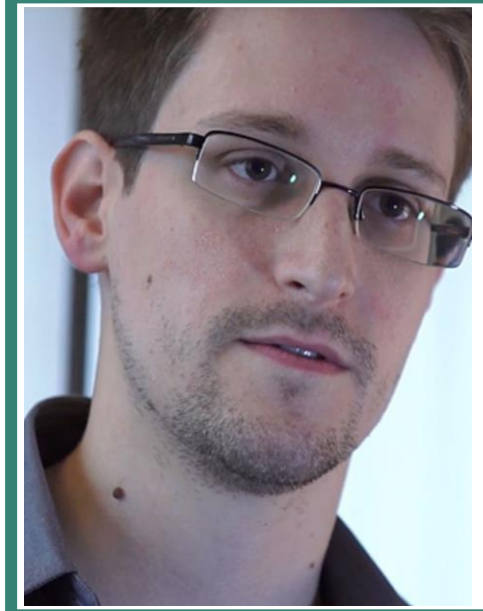
Got nothing to hide?

Are you sure?









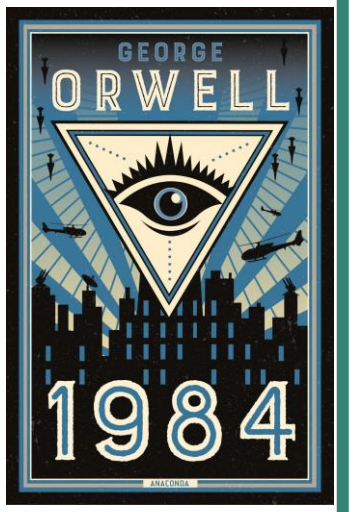
‘You simply have to eventually fall under suspicion […], even by a wrong call, and then they can use the system to go back in time and scrutinize every decision you’ve ever made, every friend you’ve ever discussed something with, and […] derive suspicion from an innocent life and paint anyone in the context of a wrongdoer.’

Edward Snowden

Why care?

Got nothing to hide?

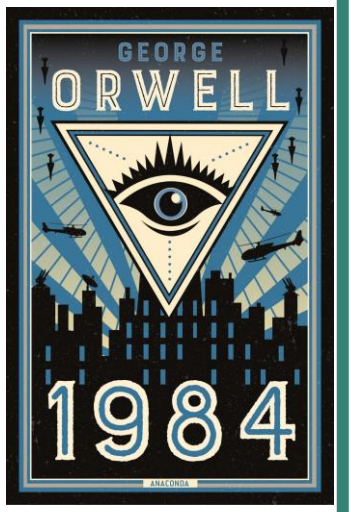
What about others?



Why care?

Got nothing to hide?

What about others?



slate.com/technology/2022/09/russia-domestic-surveillance.html

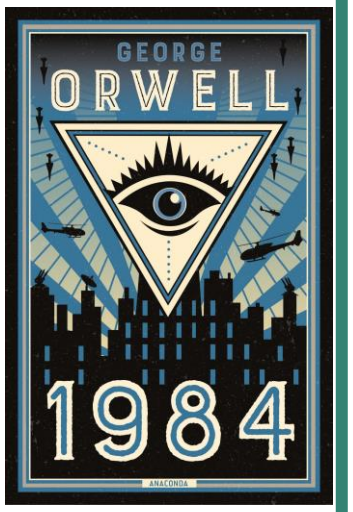
Russia Wants Citizens to Like, Comment, Subscribe for More Surveillance

BY TAMARA EVDOKIMOVA SEPT 14, 2022 • 5:50 AM

Why care?

Got nothing to hide?

What about others?



slate.com/technology/2022/09/russia-domestic-surveillance.html

Rus
Com
Surv

BY TAMARA E

eff.org

ELECTRONIC FRONTIER FOUNDATION

About Issues Our Work Take Action Tools Donate

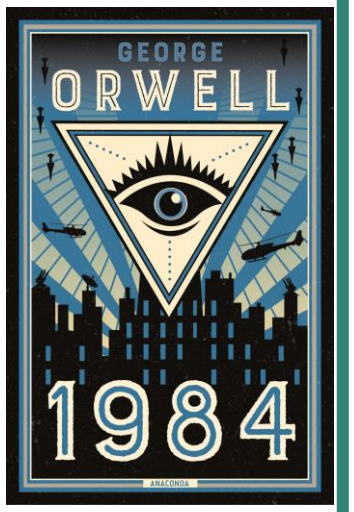
Turkey Doubles Down on Violations of Digital Privacy and Free Expression

BY KATITZA RODRIGUEZ AND HILAL TEMEL | NOVEMBER 4, 2020

Why care?

Got nothing to hide?

What about others?



slate.com/technology/2022/09/russia-domestic-surveillance.html

Rus
Con
Sur

BY TAMARA E

eff.org

ELECT
FRONT
FOL

Turkey
Expres

BY KATITZA ROD

https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html

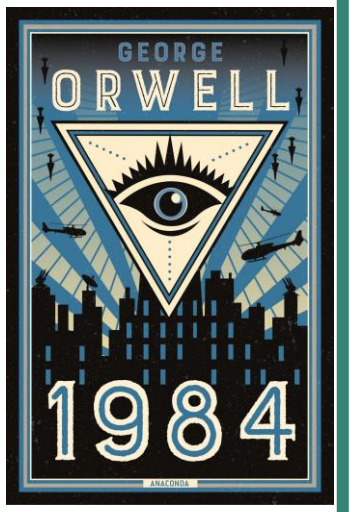
Four Takeaways From a Times Investigation Into China's Expanding Surveillance State

Times reporters spent over a year combing through government bidding documents that reveal the country's technological road map to ensure the longevity of its authoritarian rule.

Give this article 147

Why care?

Got nothing to hide?



What about others?

slate.com/technology/2022/09/russia-domestic-surveillance.html

Rus
Con
Sur
BY TAMARA E

eff.org

https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html

ELECT
FRONT
FOL

Turkey
Expres
BY KATITZA ROD

Four Takeaways From a Times Investigation Into China's Surveillance State

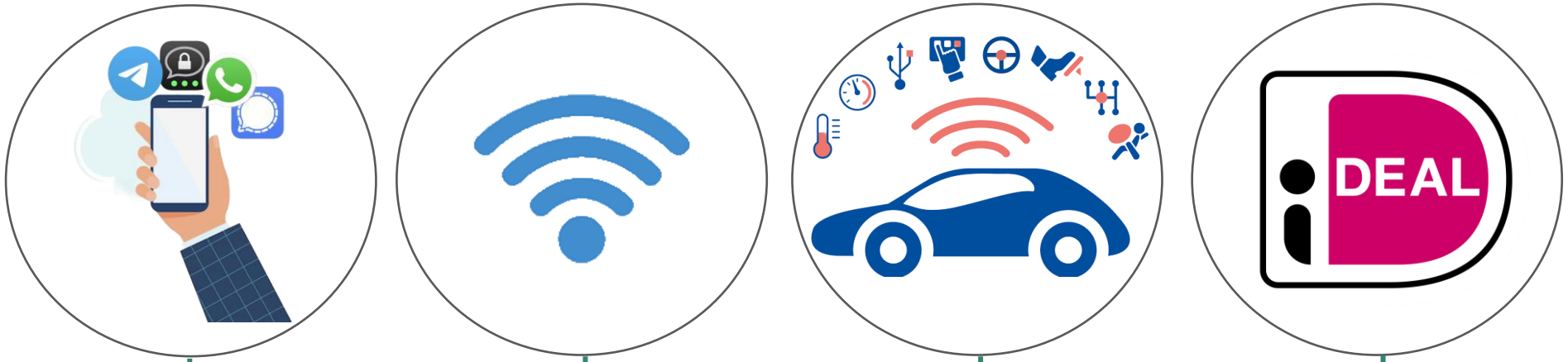
Times reporters spent over a year combing
bidding documents that reveal the country
map to ensure the longevity of its authorita

Give this article 147

Online anonymity project:

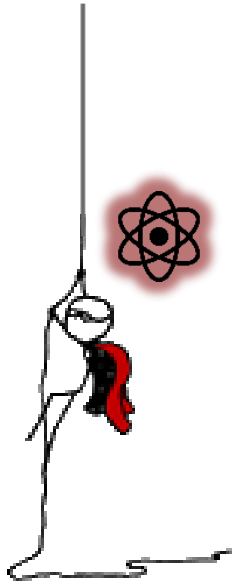
‚Quantum kills the internet‘

‚Quantum kills the internet‘



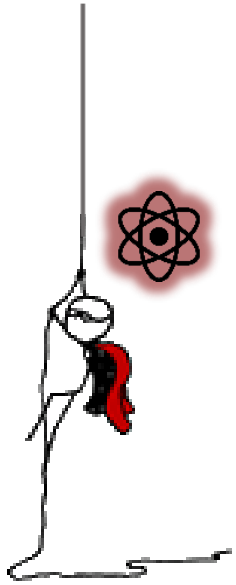
Uses public-key crypto (Rivest-Shamir-Adleman, Diffie-Hellman)

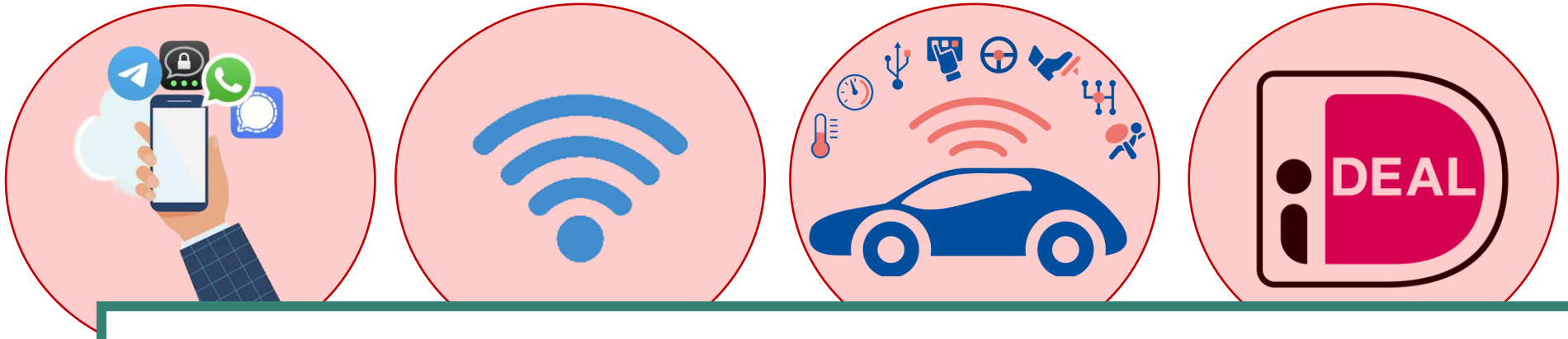
‚Quantum kills the internet‘



Uses public-key crypto (Rivest-Shamir-Adleman, Diffie-Hellman)

‚Quantum kills the internet‘





What exactly goes wrong?

Uses public-key crypto (Rivest-Shamir-Adleman, Diffie-Hellman)

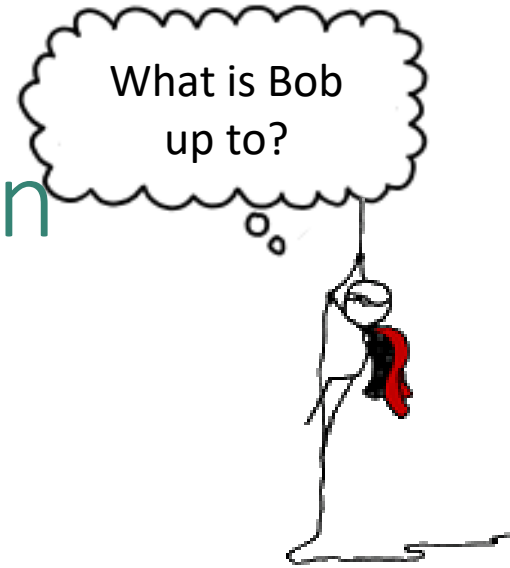
Rivest-Shamir-Adleman (RSA) encryption

Alice

Bob

Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption

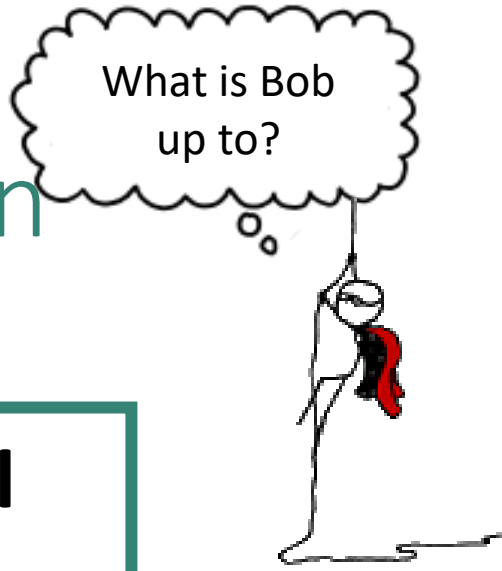


Alice

Bob

Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption



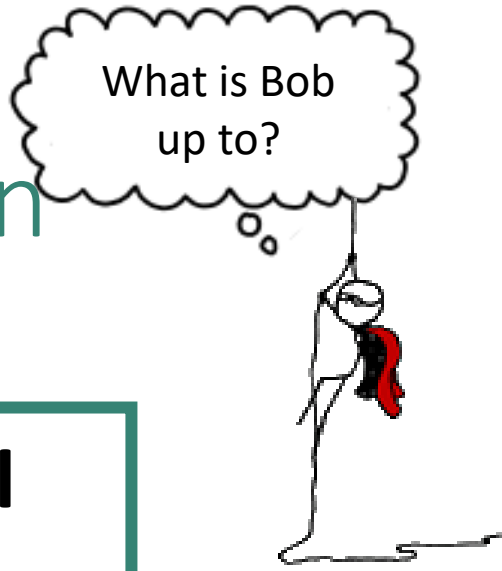
Alice

How can Alice safely tell Bob to sell over the internet?

Bob

Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption



Alice

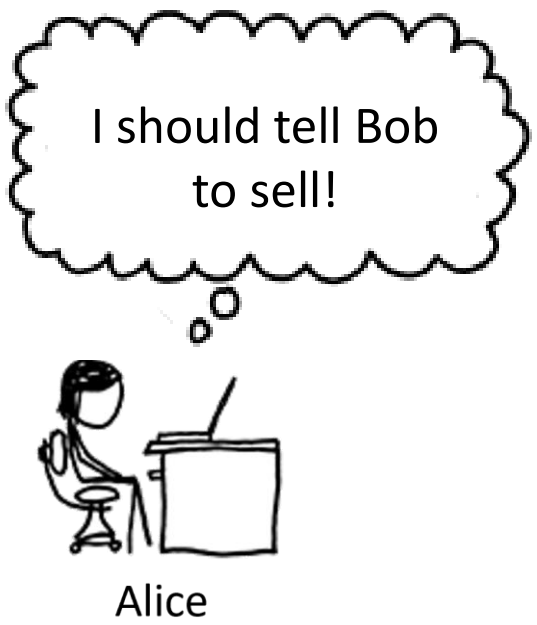
How can Alice safely tell Bob to sell over the internet?

Computations with primes!

Bob

Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption



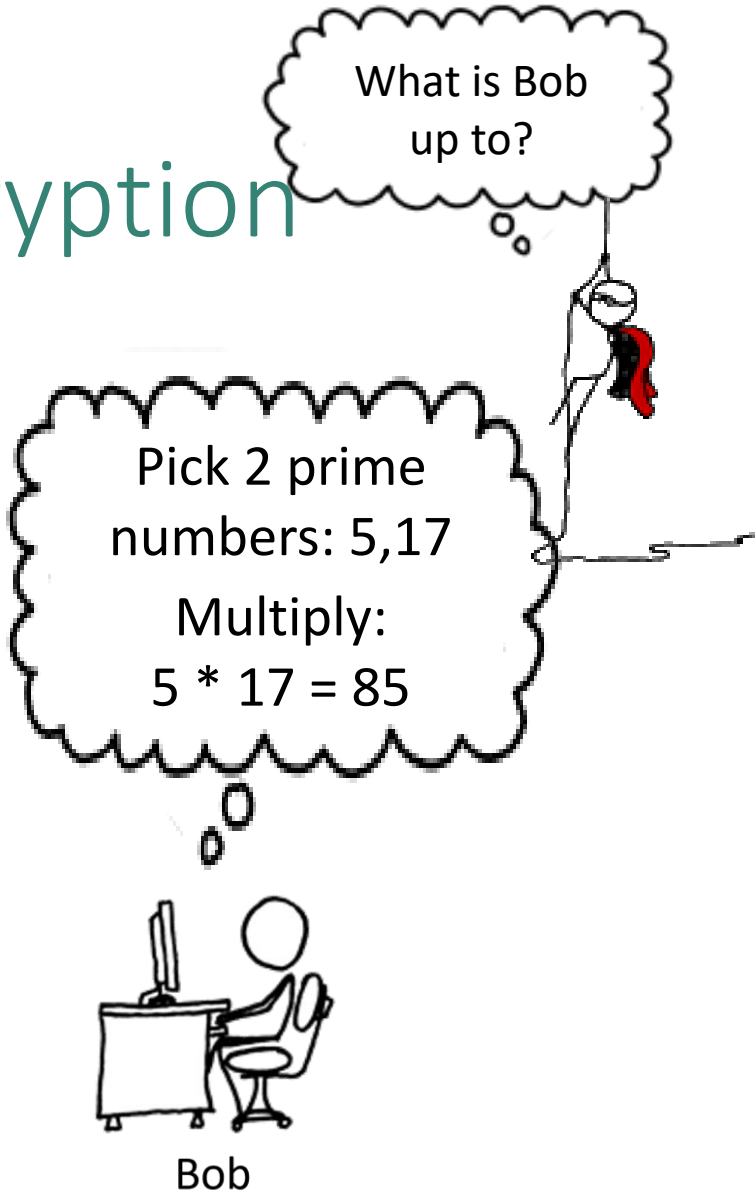


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption

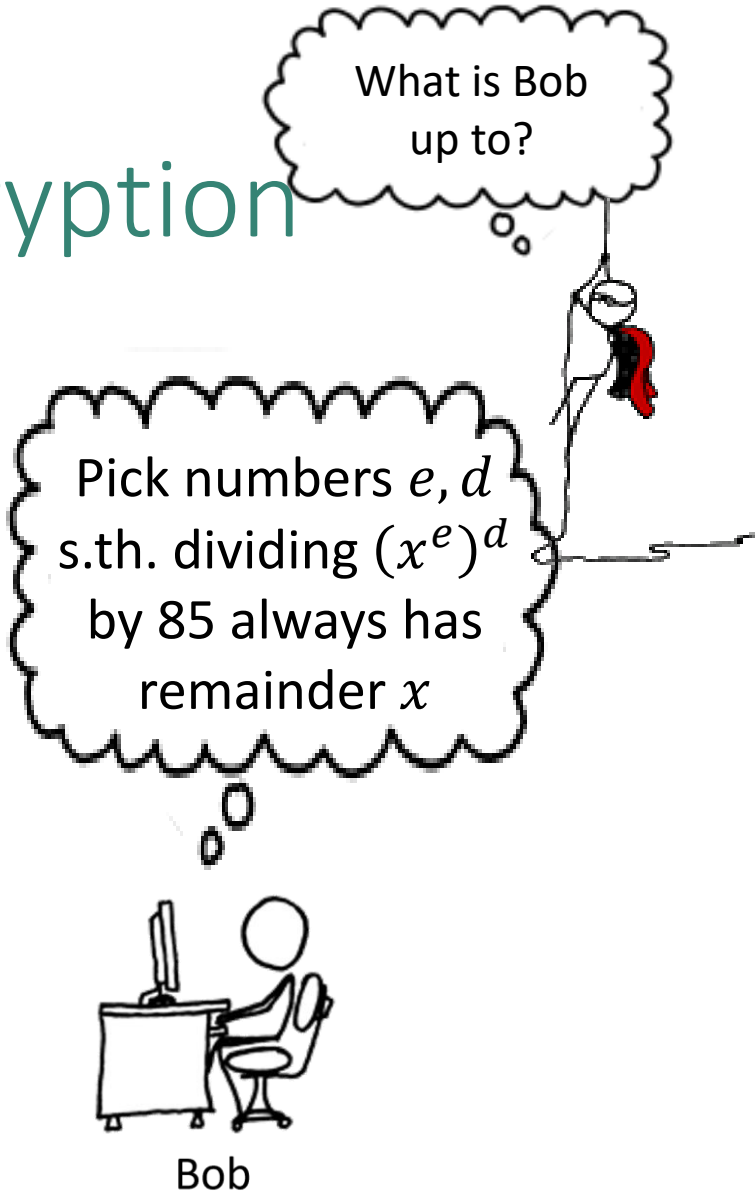


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption

Example:

$e = 5, d = 13$

$x = 2$

$x^e = 2^5 = 32$

$(2^e)^d = 32^{13}$ (large, but has remainder 2!)

Also works for $x = 3, x = 4, x = 5, \ldots$

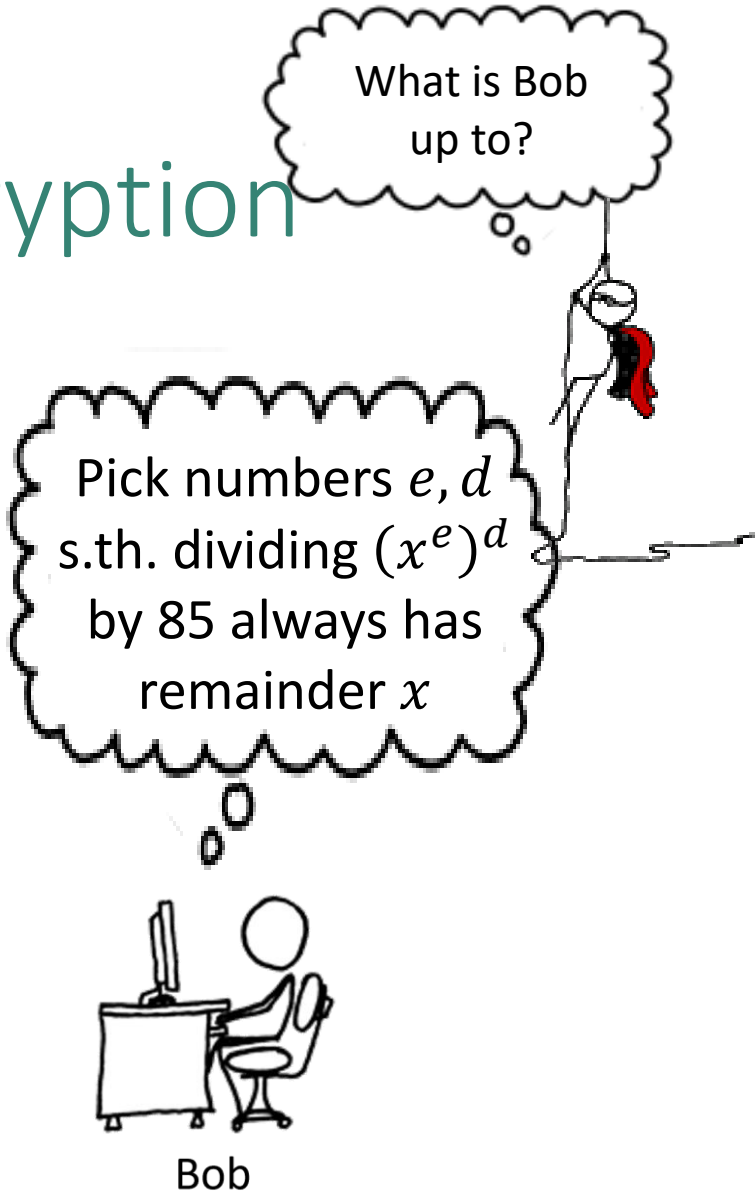


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption

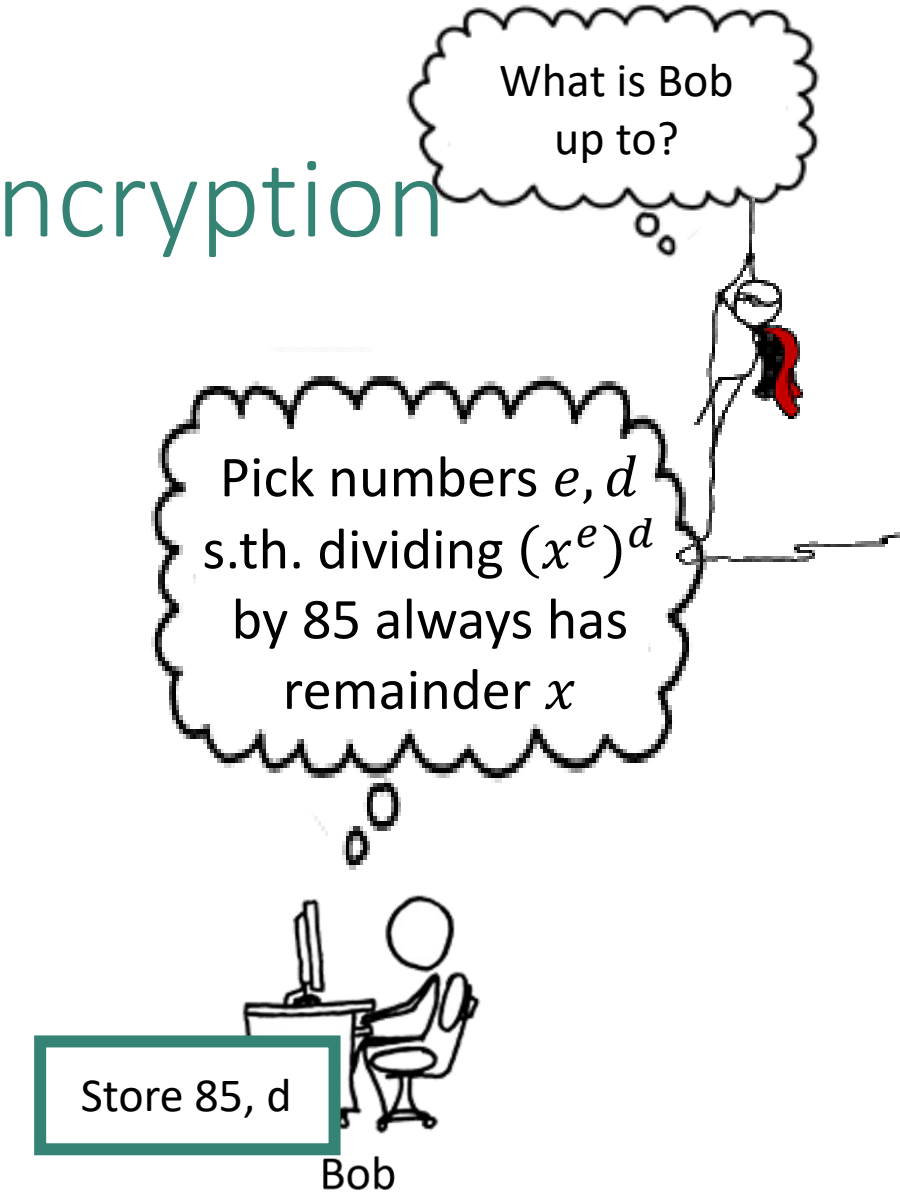


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption

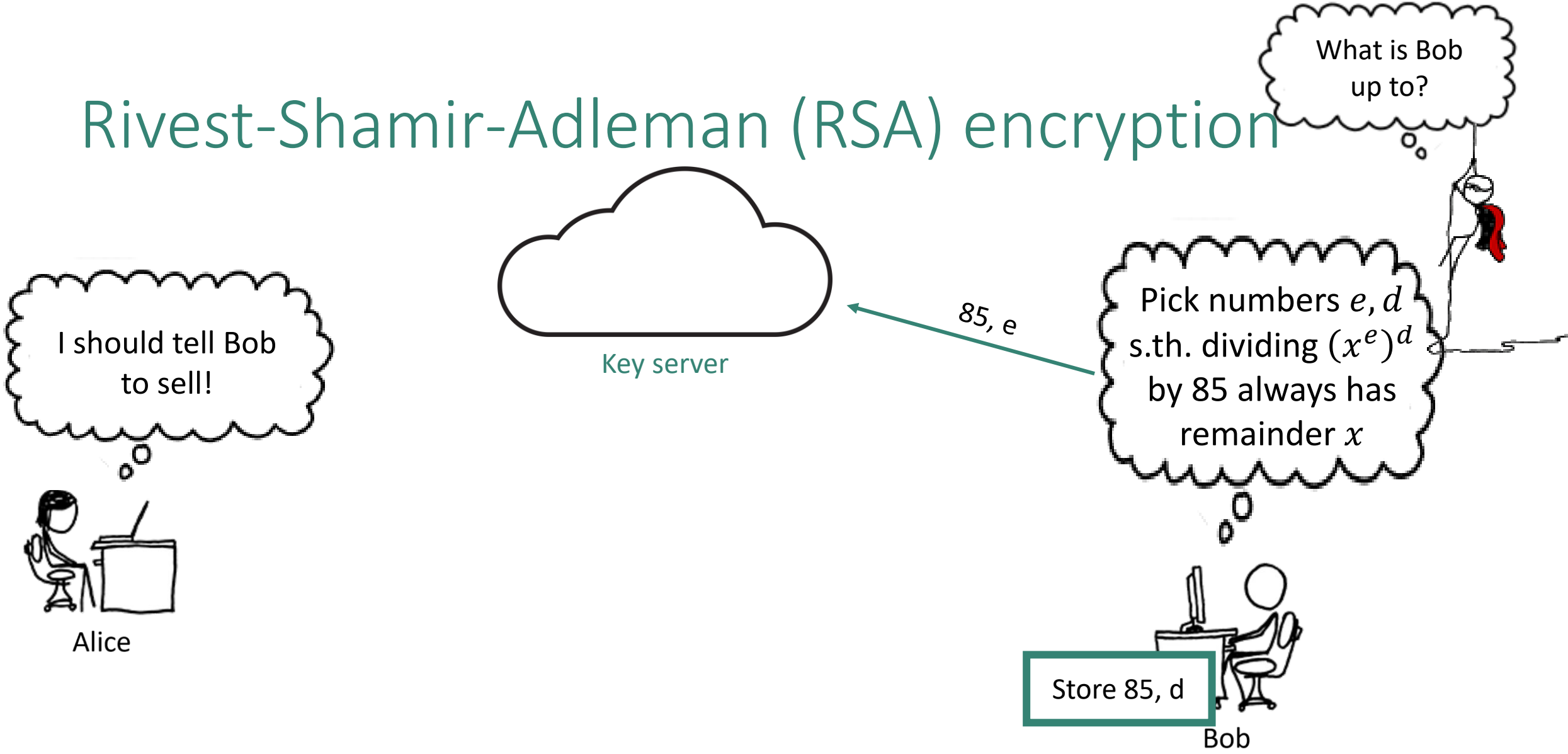


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption

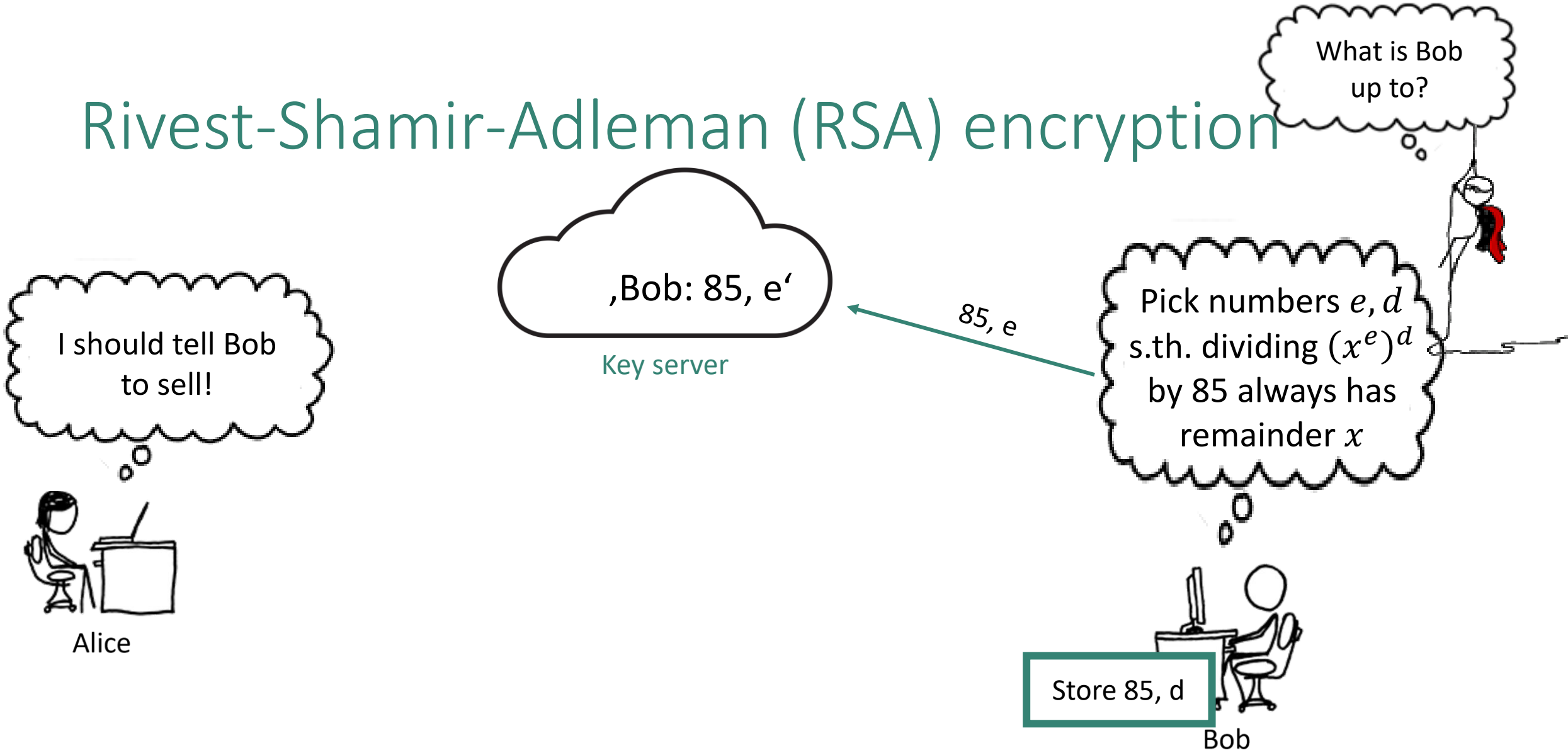


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption

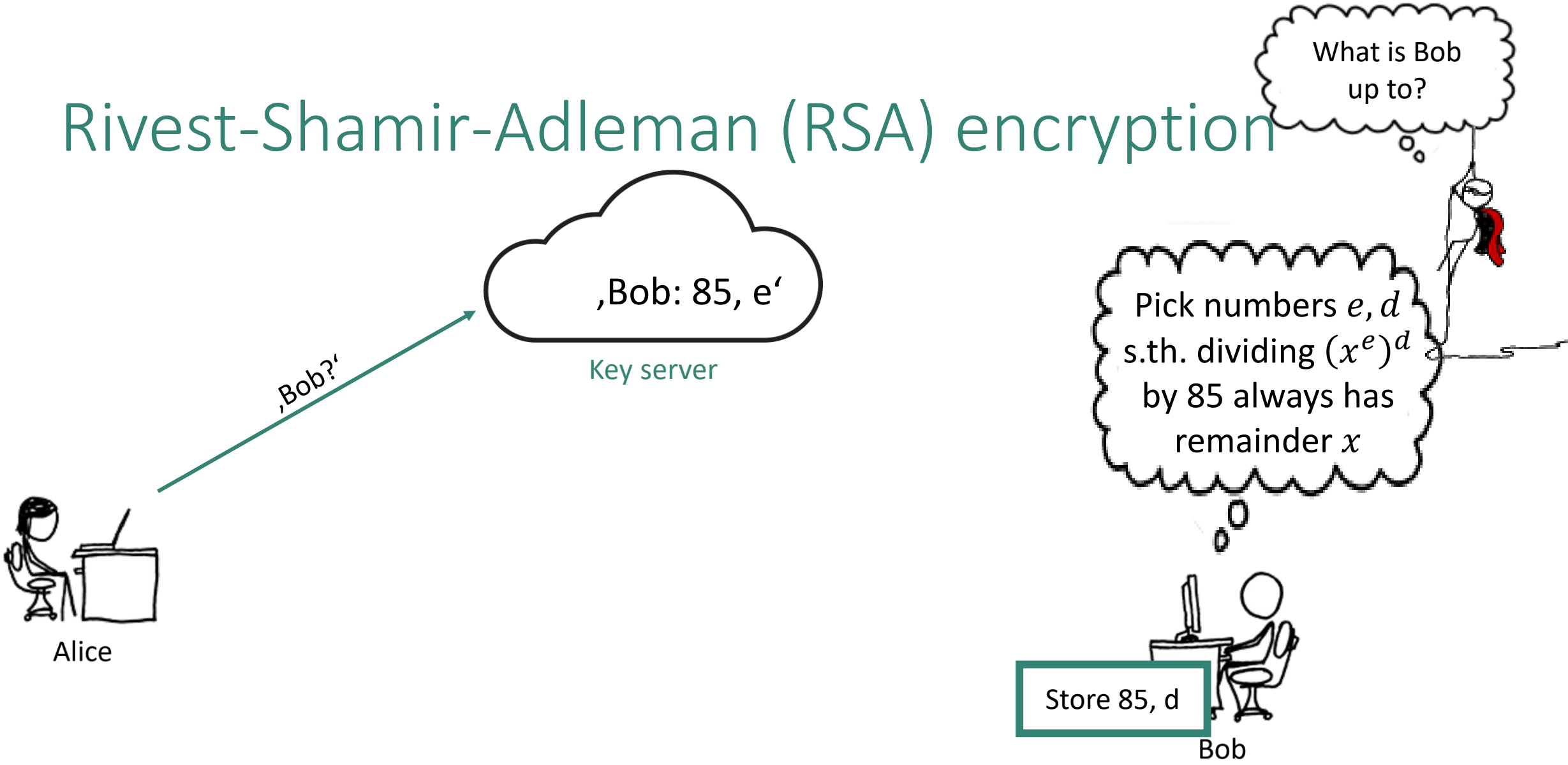
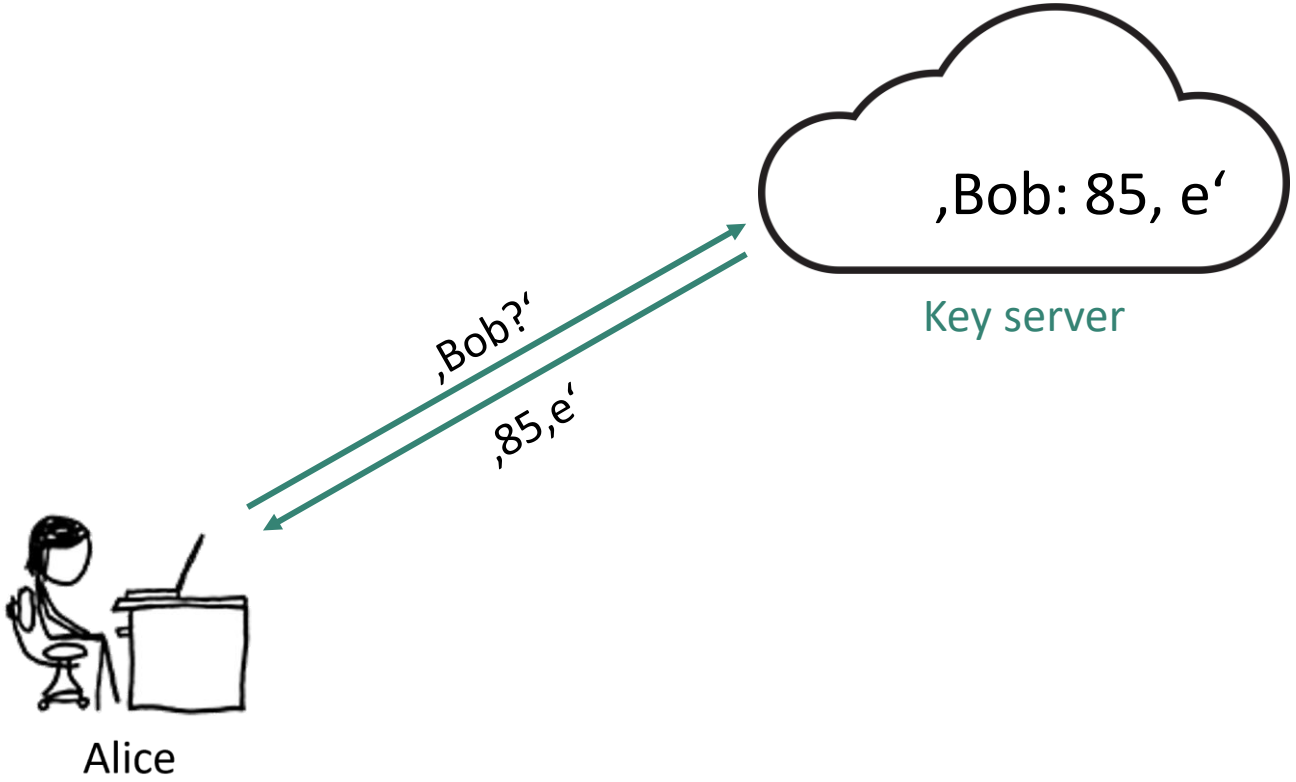


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption



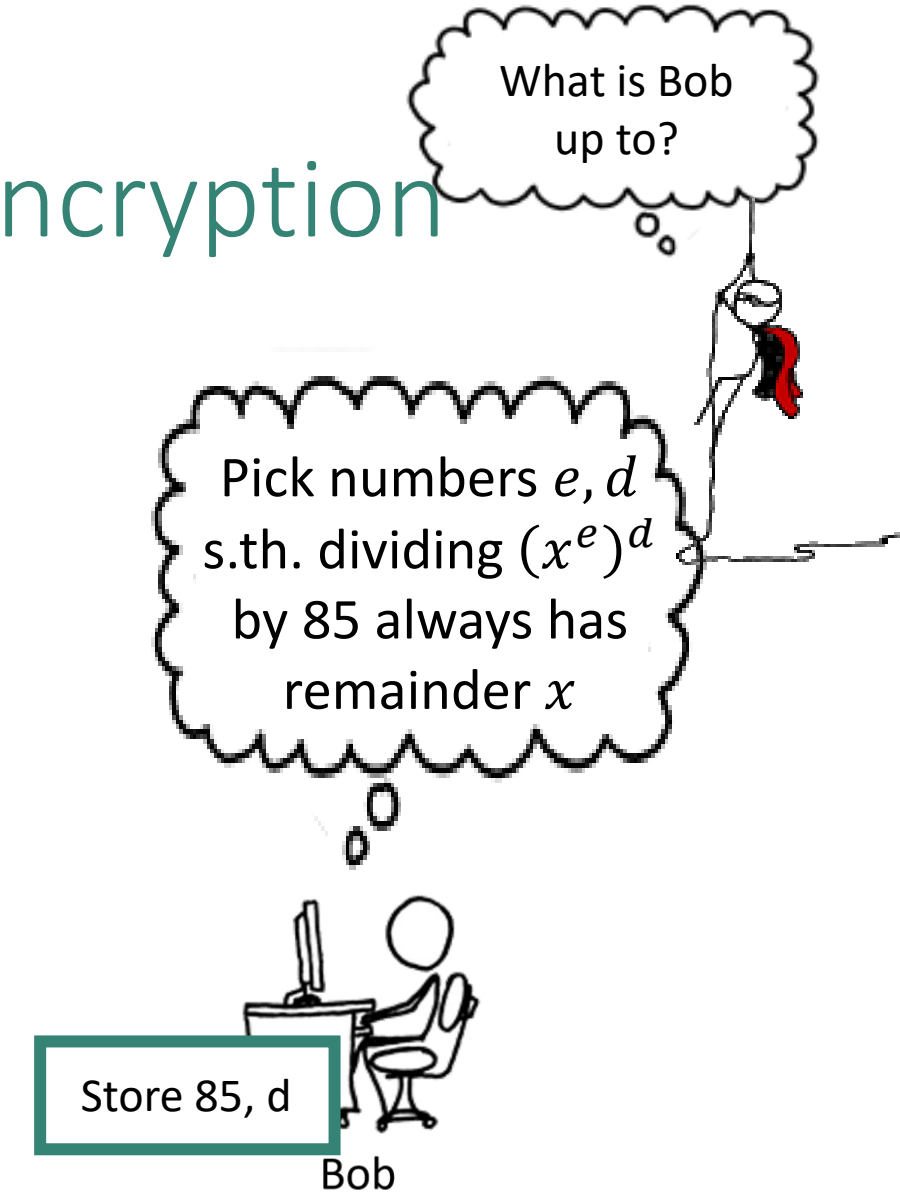
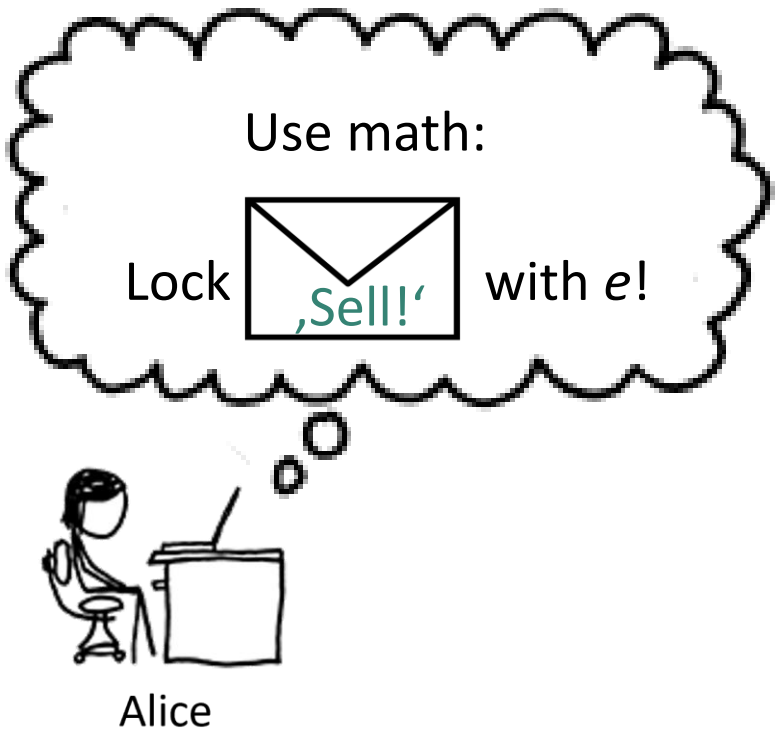


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption



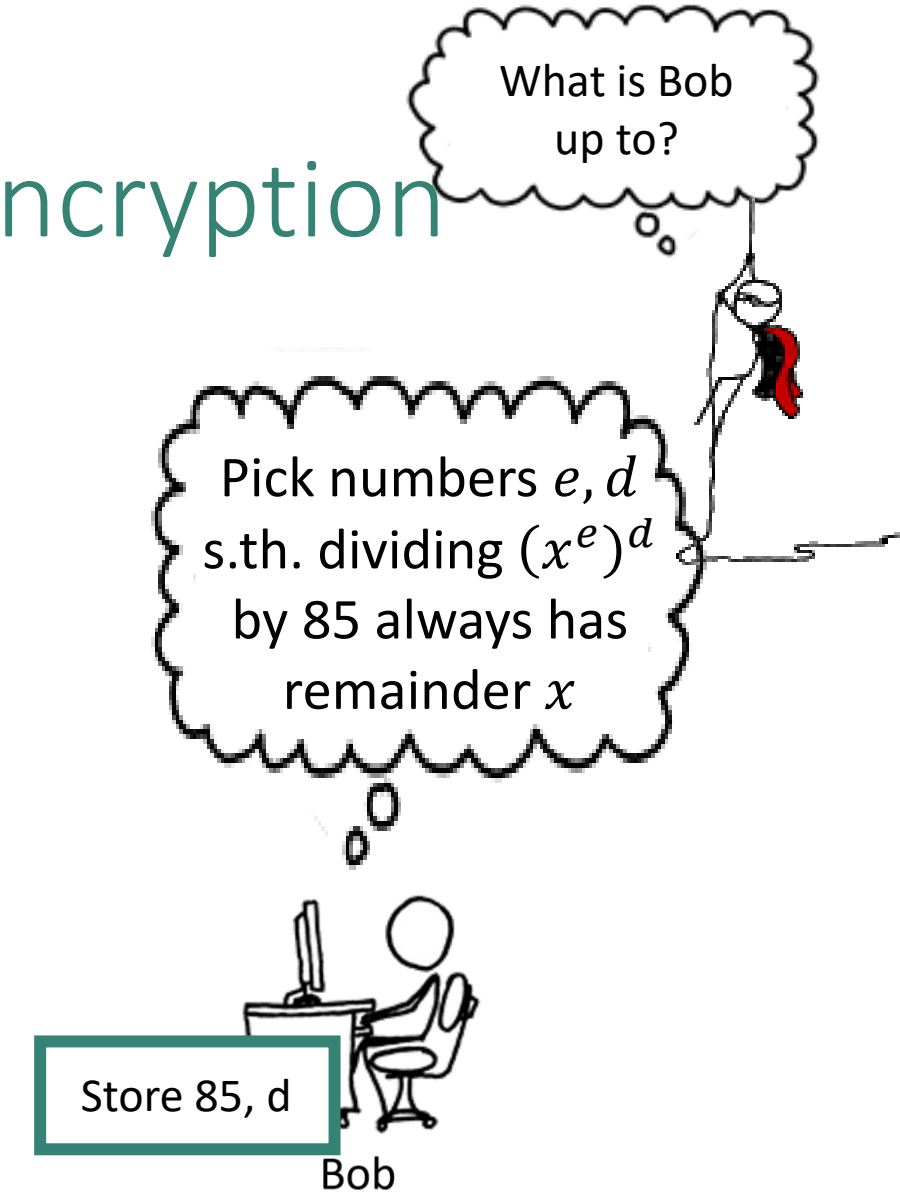
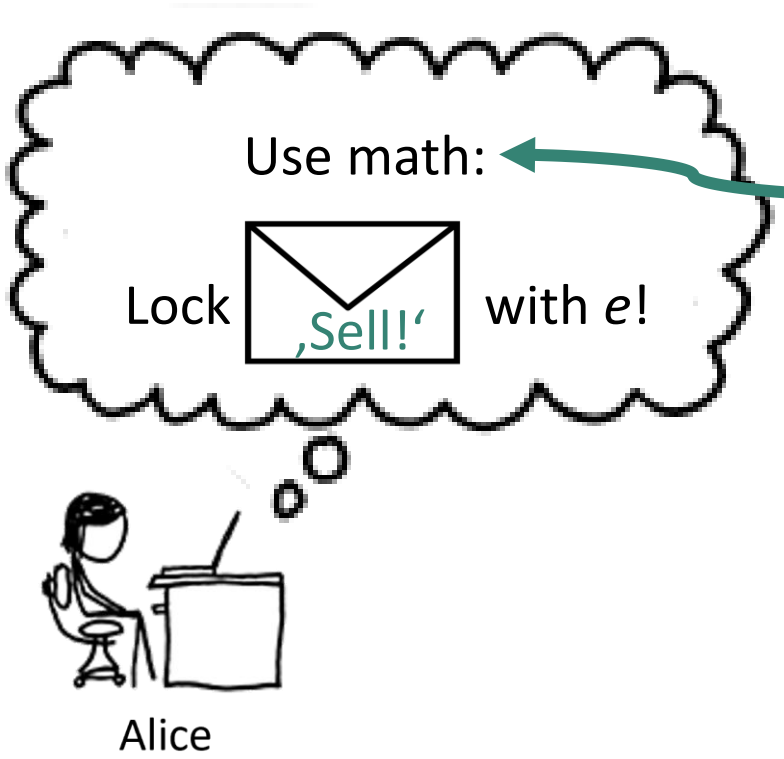


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption



The math:

Convert ‚Sell‘ to a number $m < 85$

Compute m^e

Divide by 85, keep the remainder

Use the remainder as ‚Sell!‘

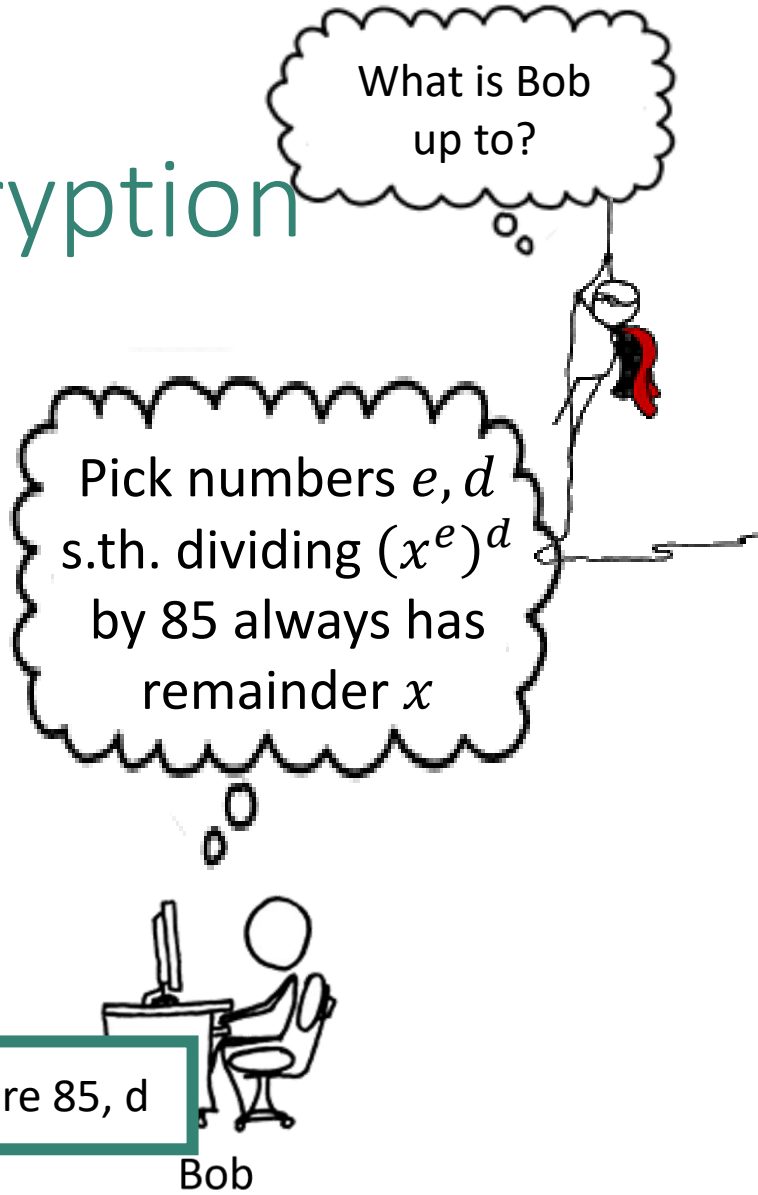


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption

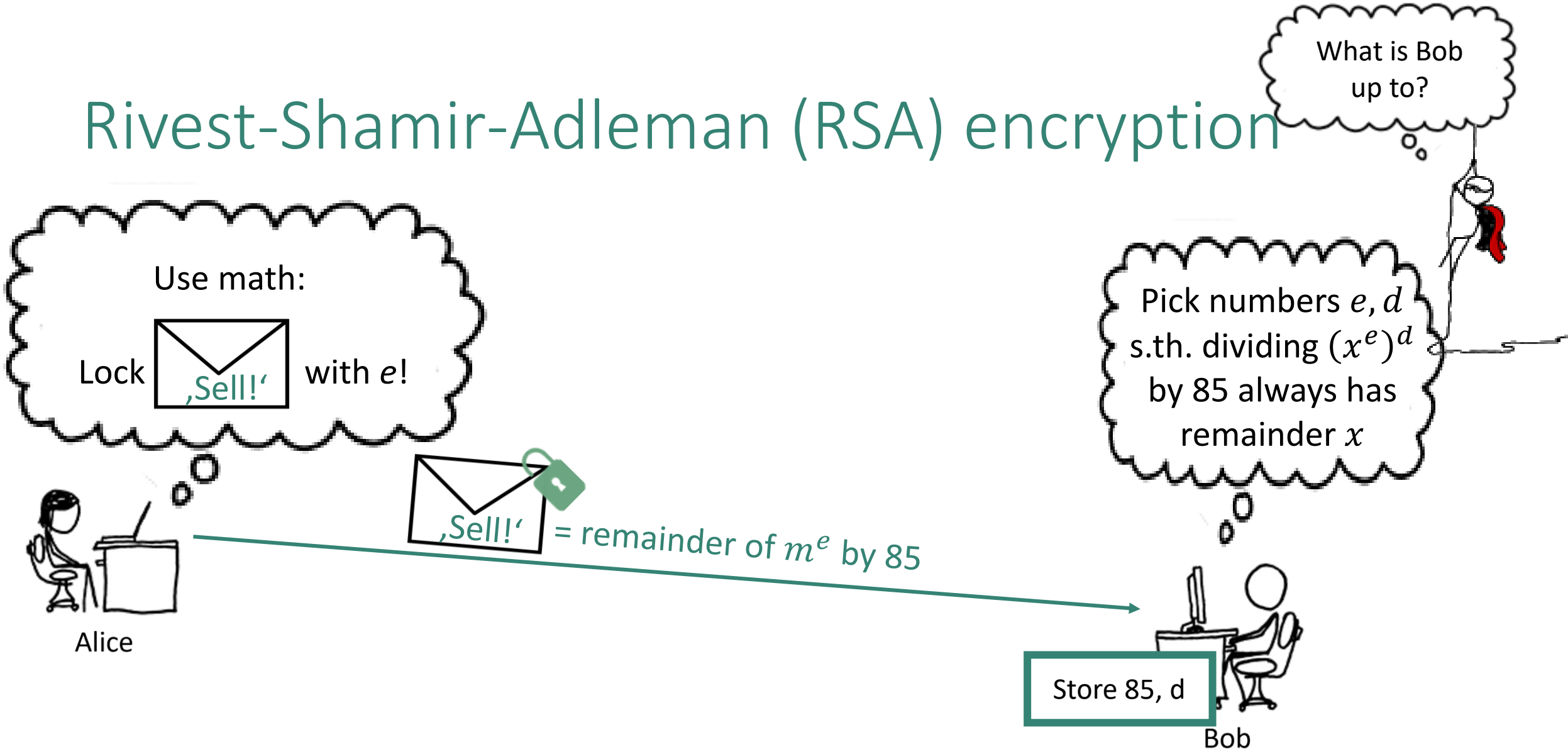
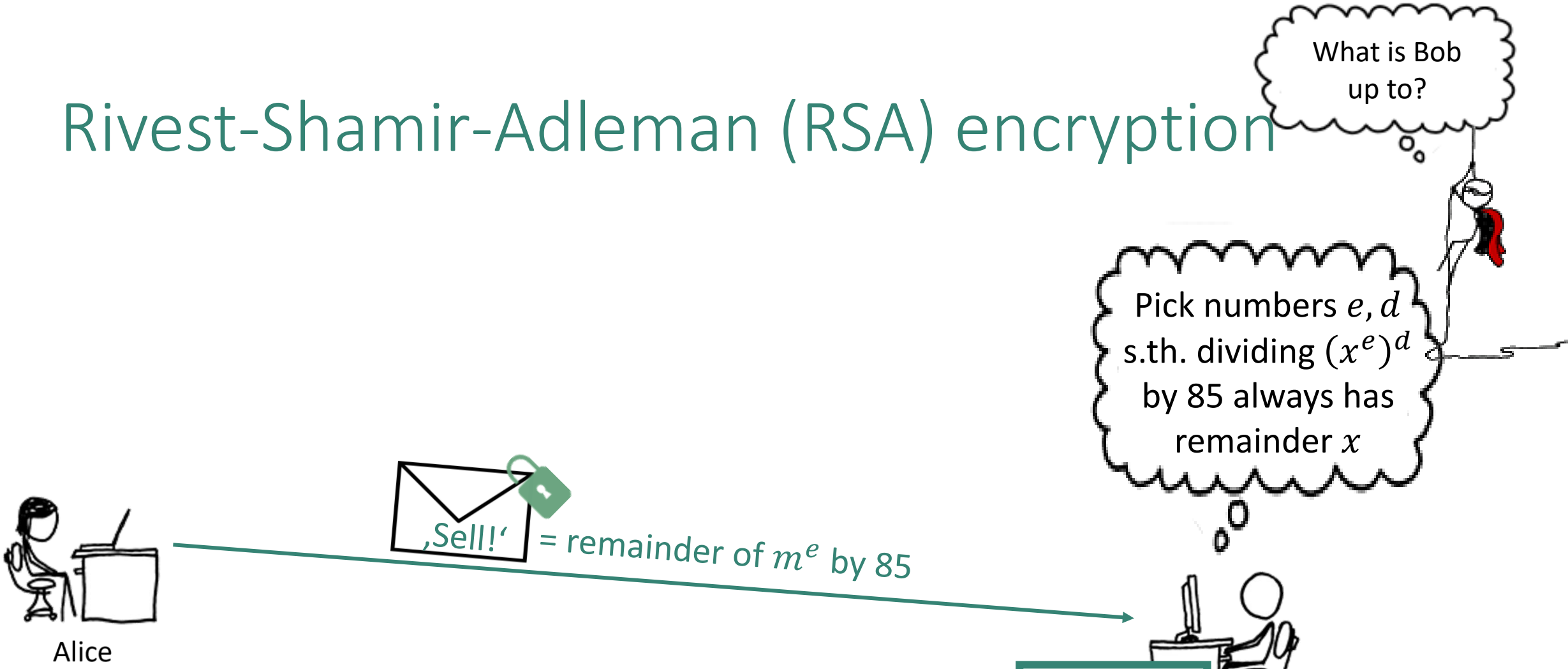


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption



Unlocking

message $m = remainder(m^e)^d$

Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption

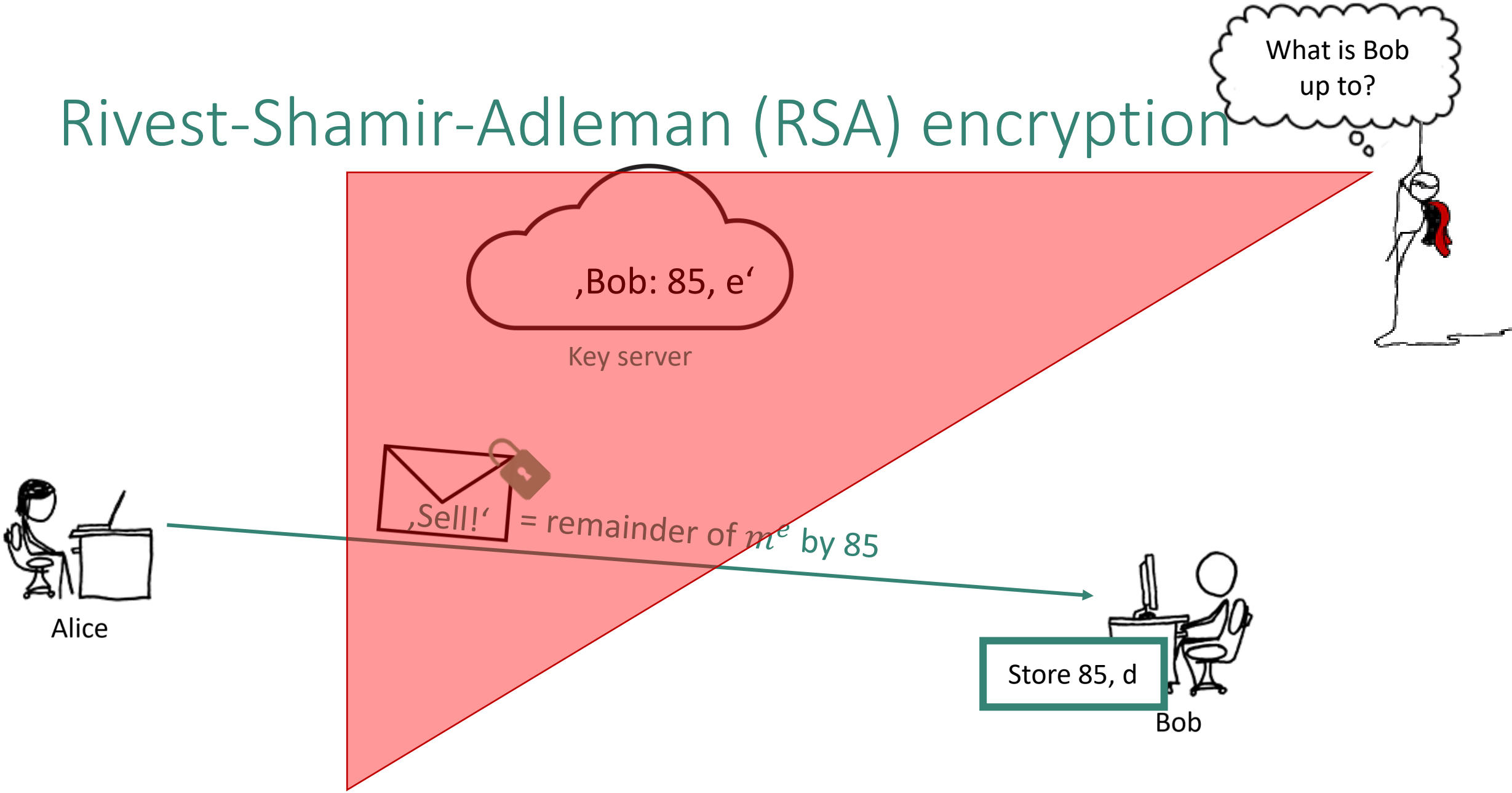


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption

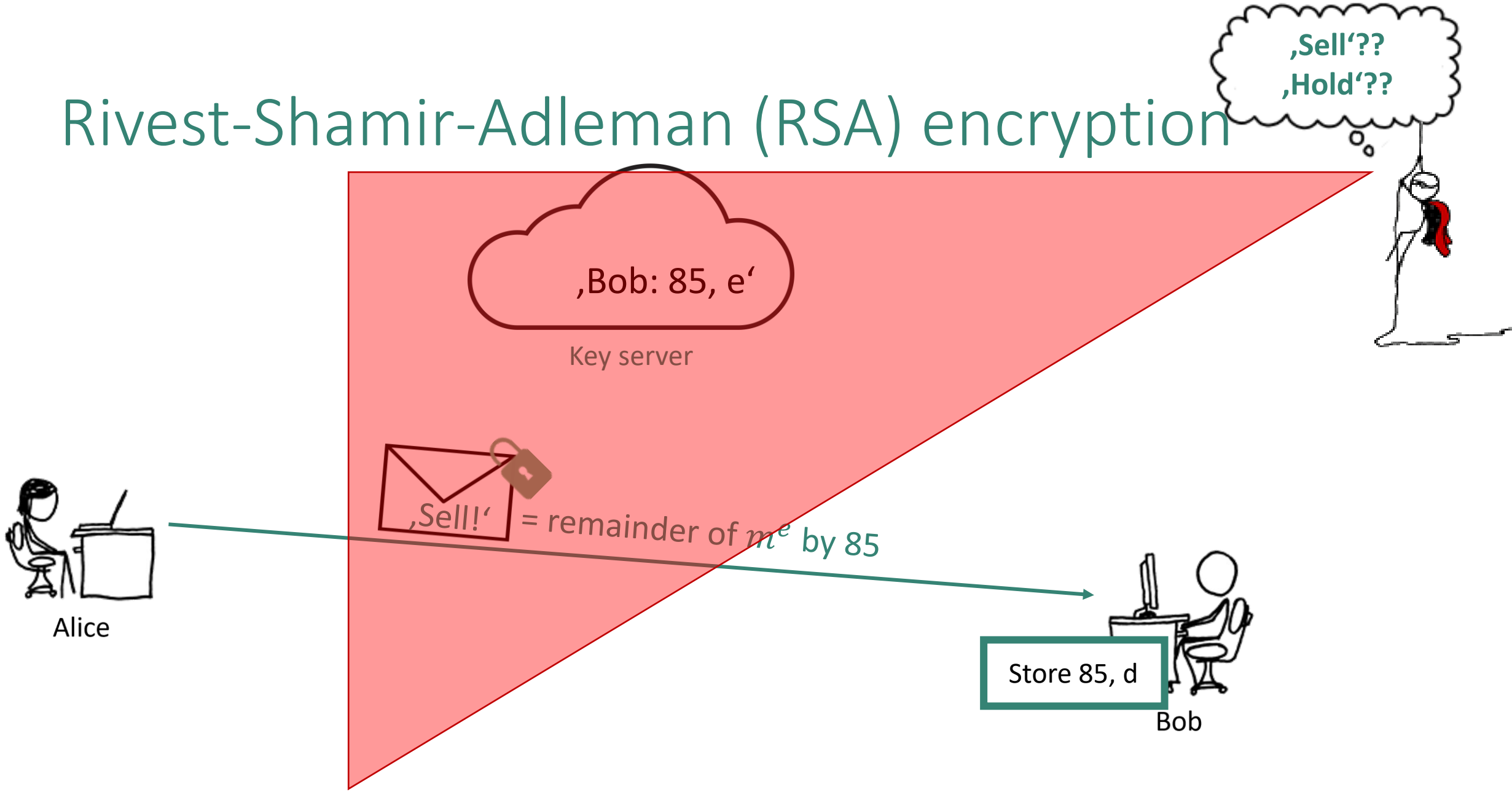
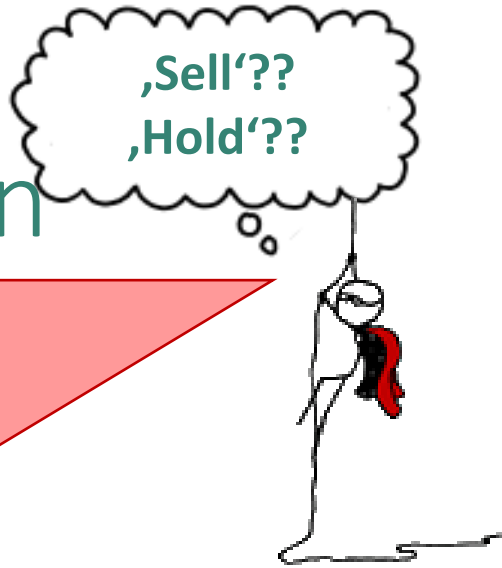
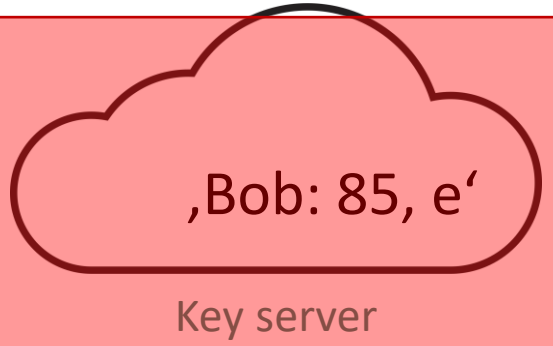


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption





Breaking 

is as hard as factoring 85 into 5 and 17

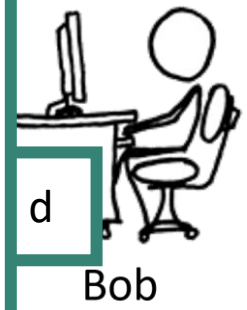
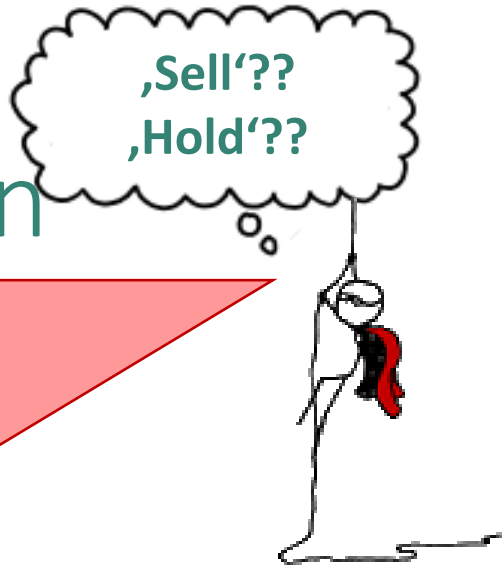
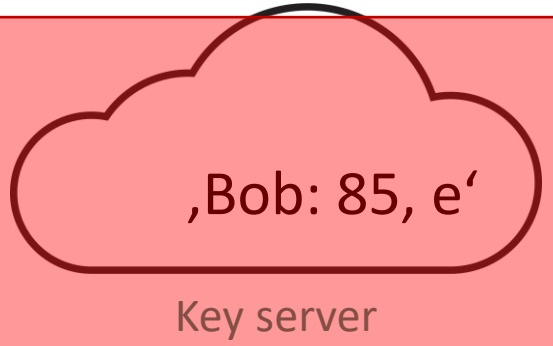


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption





Breaking 

is as hard as factoring 85 into 5 and 17

Wait, is that hard…?

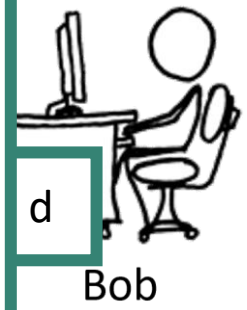
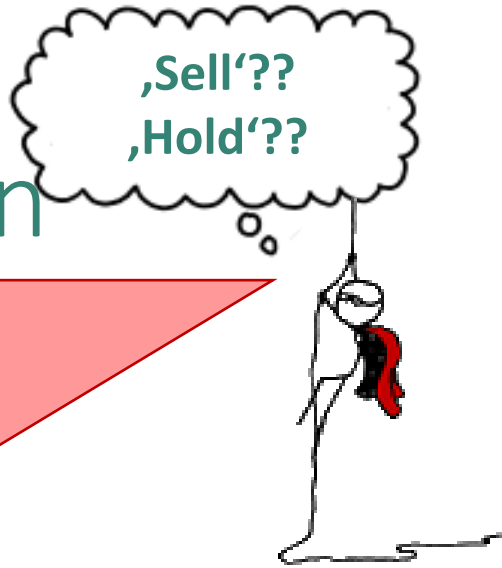
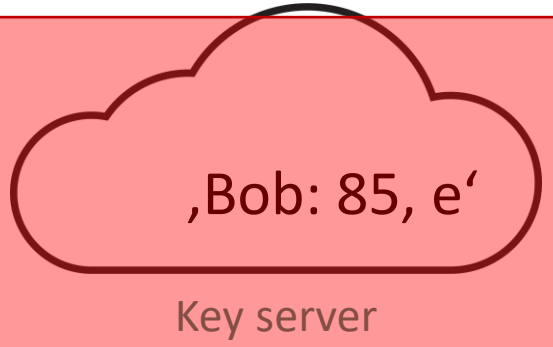


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption





Breaking 

is as hard as factoring 85 into 5 and 17

Wait, is that hard…?

Use BIG prime products (> 2048 digits)

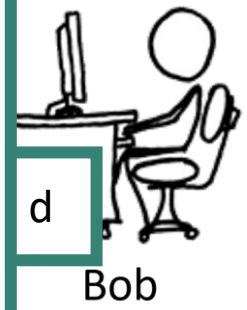
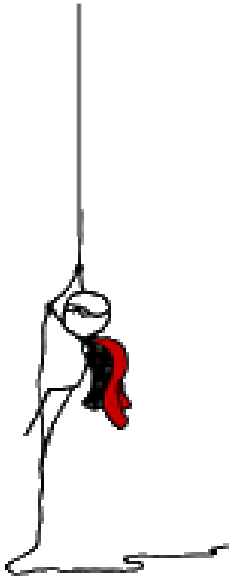


Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption



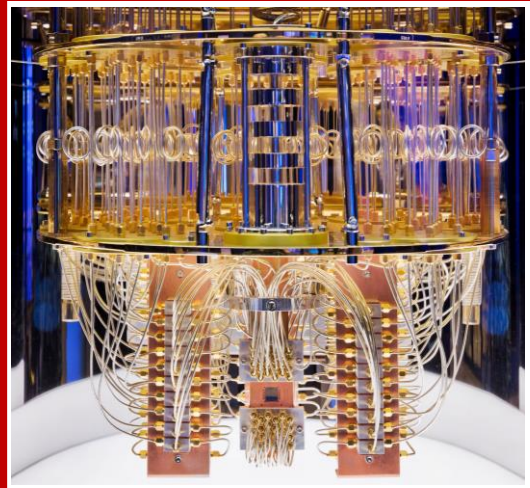
Take-away:

RSA idea: multiplying is easy, but factoring is hard.

Use BIG prime products (> 2048 digits)

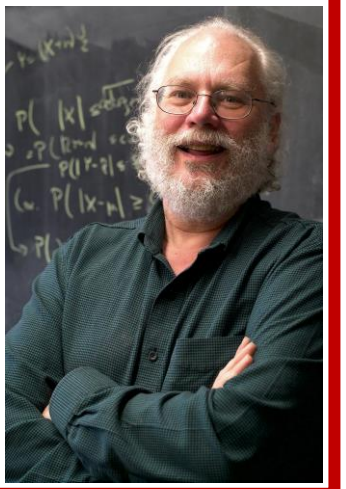
Image source: xkcd.com

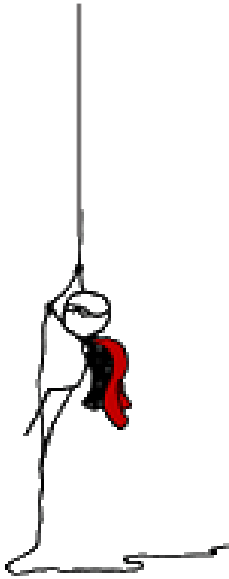
Rivest-Shamir-Adleman (RSA) encryption



Shor, 1994:

Large quantum computers: (essentially) factor as fast as they multiply.



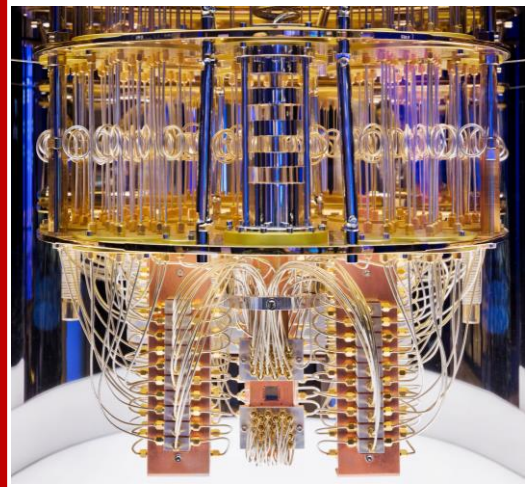


RSA idea: multiplying is easy, but factoring is hard.

Use BIG prime products (> 2048 digits)

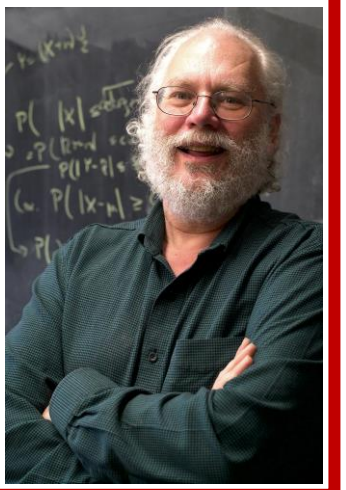
Image source: xkcd.com

Rivest-Shamir-Adleman (RSA) encryption



Shor, 1994:

Large quantum computers: (essentially) factor as fast as they multiply.



~~RSA idea~~: multiplying is easy, but factoring is hard.

Use BIG prime products (> 2048 digits)

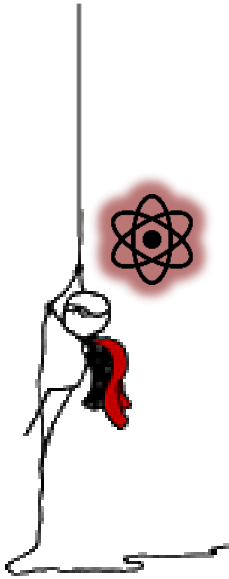
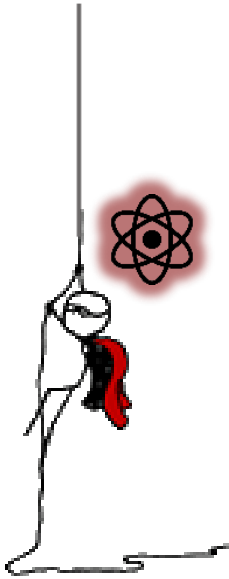
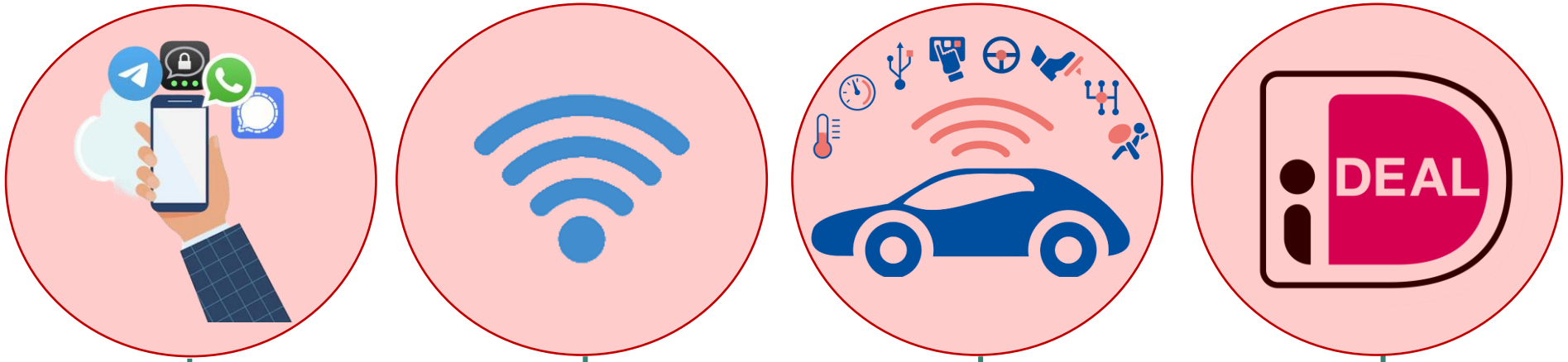


Image source: xkcd.com

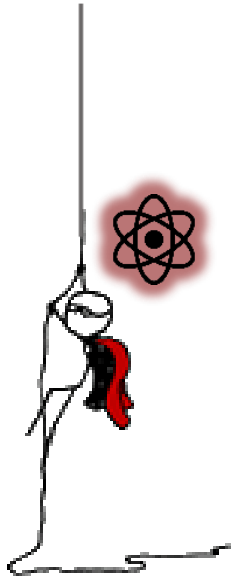
‚Quantum kills the internet‘





Uses public-key crypto (Rivest-Shamir-Adleman, Diffie-Hellman)

Should we worry?



x = time needed to migrate

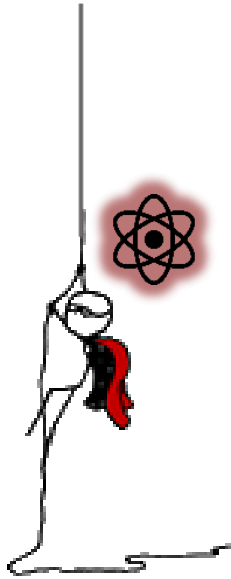
y = security shelf life

z = time to break system

Secret keys leaked

If $x + y > z$ then worry

Should we worry?



x = time needed to migrate

y = security shelf life

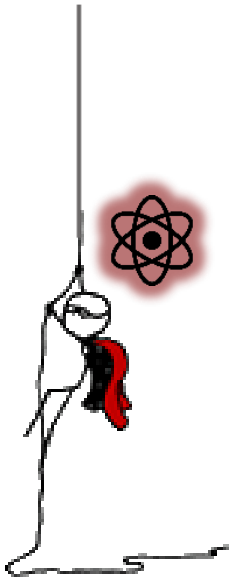
z = time to break system

Secret keys leaked

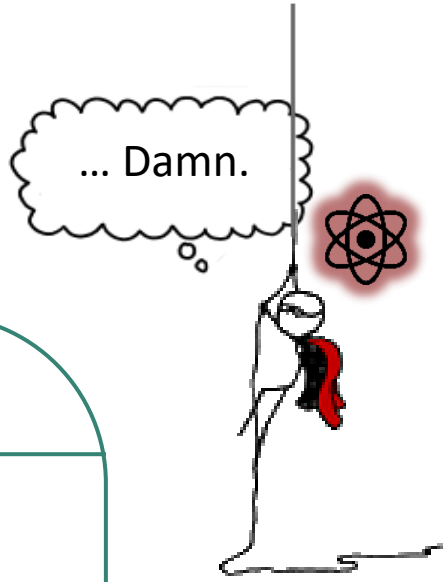
If $x + y > z$ then worry

'record now, break later' ⇒ **today's** data

Hm… And now?



Hm… And now?



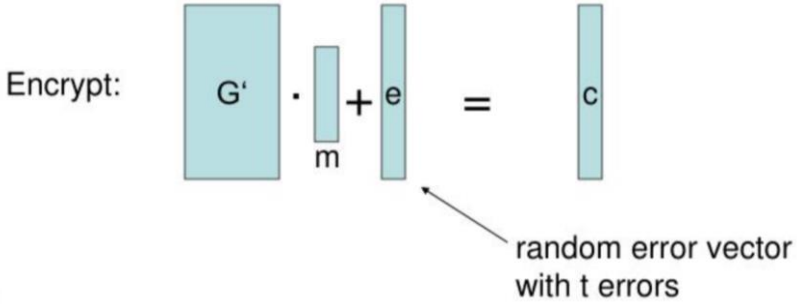
~~Factoring~~ Something that's hard even for quantum computers

Finding a shortest vector in a lattice

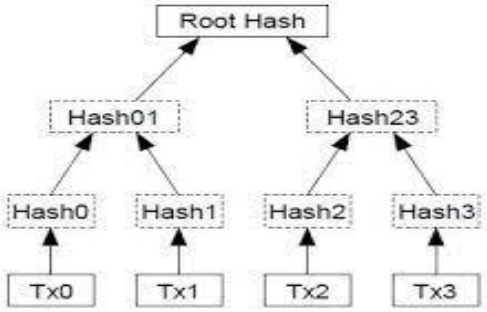
$$1000\,x + x^2 + 423\,y^2 z = 1$$
$$655\,y + 53\,yz = 13$$
$$29\,x + 3\,y^2 + 53\,xz^2 = 4$$

Solving polynomial equations with > 1 variables

Decoding error-correcting codes



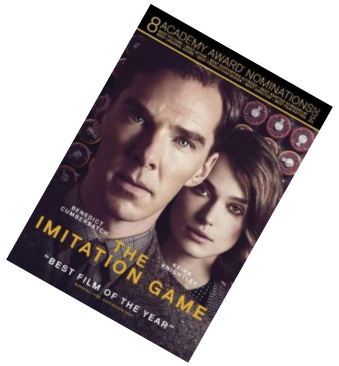
Finding collisions, preimages… in hash functions



Thanks for listening!

kathrin@hoevelmanns.net
Twitter: @quantum_bat

Like math and computer science? Look up (post-)quantum crypto!



Watch *The imitation game*.

Read Orwell's *1984*.

Help out the TOR project. (No crypto knowledge needed!)

Political aspects of crypto: 'Crypto wars' on Wikipedia.