EXPLORING CRYPTOGRAPHY PROTOCOLS

WITH LIMITED EMPHASIS ON MATHEMATICS ☺

Presented By
@7eRoM

ATTENTION

THESE SLIDES HAVE BEEN CRAFTED USING THE FOUNDATION OF MY MSC COURSE IN CRYPTOGRAPHY PROTOCOLS AT THE UNIVERSITY OF ISFAHAN.

I'VE MADE ADJUSTMENTS TO THE CONTENT TO ALIGN WITH THE SPECIFIC OBJECTIVES OF THIS PRESENTATION.

ALSO, MY INTENTION HAS BEEN TO MINIMIZE THE USE OF MATHEMATICAL CONCEPTS, WHICH MAY RESULT IN SOME CONCEPTS BEING SIMPLIFIED OR LESS PRECISE.

Presented By
@7eRoM

Agenda

1. Identification and Entity Authentications Protocols
2. Zero Knowledge Protocols
3. Key Establishment Protocols
4. Threshold Cryptography and Secret Sharing Protocols
5. Types of Digital Signatures
6. Special Purpose Protocols (like simultaneous contract signing, mental poker, fair exchange)
7. Identity Based Cryptography
8. Secure Auctions and Elections Protocols
9. Cryptocurrency
10. Secure Multiparty Computations

Agenda

1. Identification and Entity Authentications Protocols
2. Zero Knowledge Protocols
3. Key Establishment Protocols
4. Threshold Cryptography and Secret Sharing Protocols
5. Types of Digital Signatures
6. Special Purpose Protocols (like simultaneous contract signing, mental poker, fair exchange)
7. Identity Based Cryptography
8. Secure Auctions and Elections Protocols
9. Cryptocurrency
10. Secure Multiparty Computations

Levels of Authentications

- Weak Authentication (based on password)
- Strong Authentication (based on challenge and response)
- Extremely Strong Authentication (based on zero knowledge)

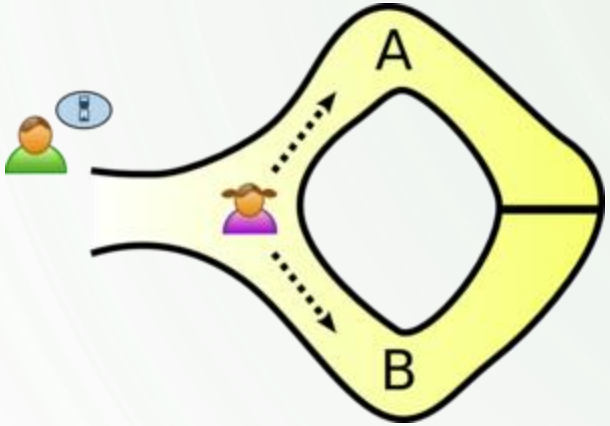
Extremely Strong Authentication

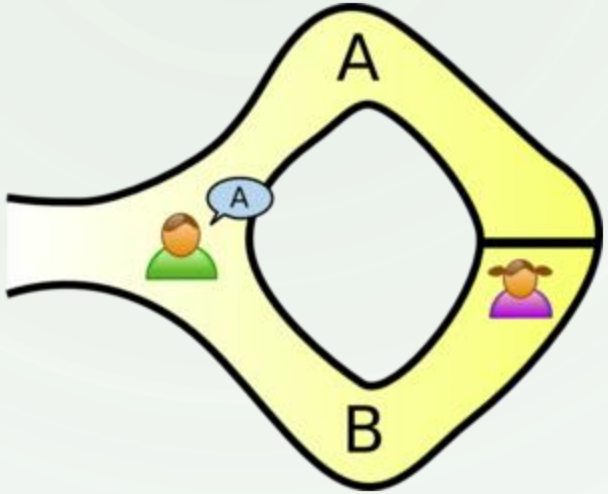
Zero Knowledge

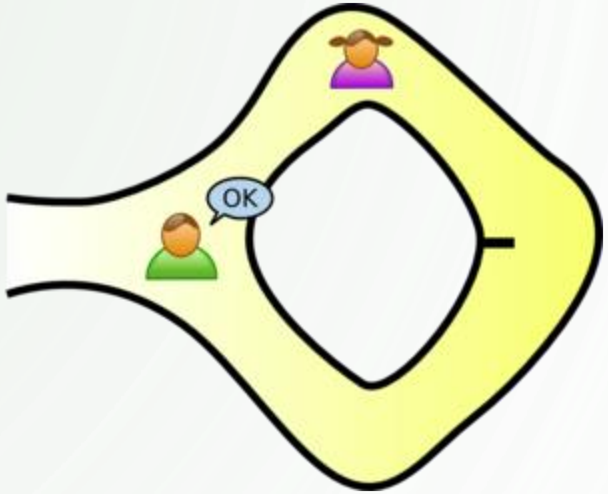
Refers to a protocol or proof in which one party, called the **prover**, can demonstrate knowledge of a certain piece of information to another party, called the **verifier**, without revealing any additional information beyond the validity of the statement.

Extremely Strong Authentication

Alibaba Cave







Peggy has the secret word used to open a magic door.

Peggy randomly takes either path A or B, while Victor waits outside

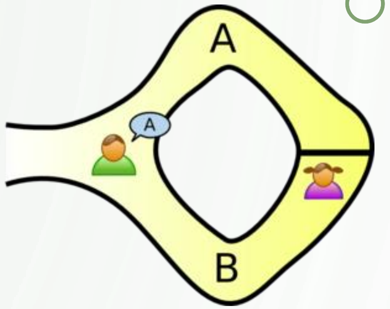
Victor enters the cave and shouts the name of the path he wants her to use to return, either A or B, chosen at random

Peggy reliably appears at the exit Victor names.

If Peggy repeatedly do that, he can conclude that it is extremely probable that Peggy know the secret word.

Extremely Strong Authentication

Alibaba Cave

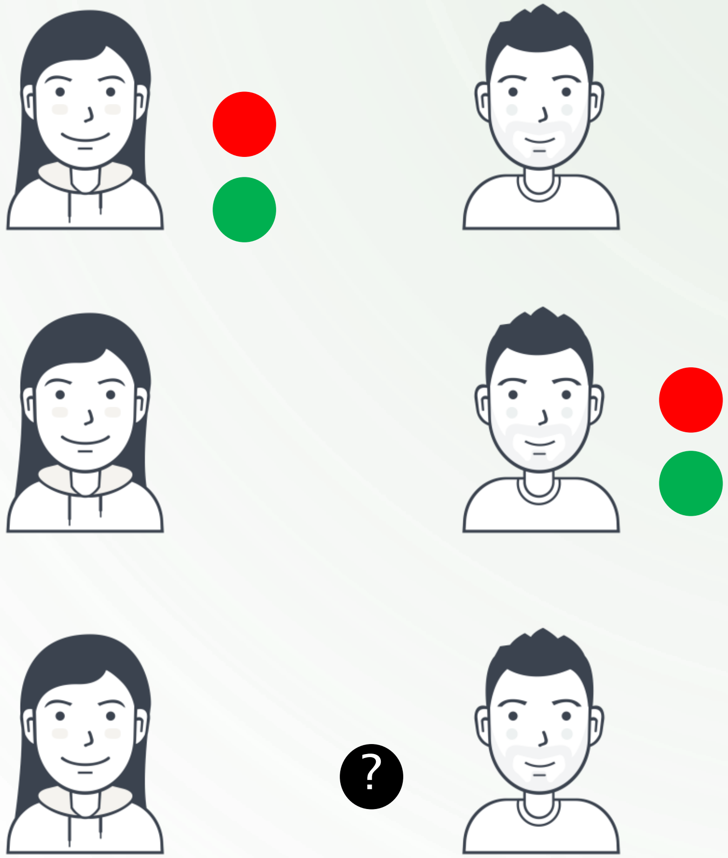


- suppose she did not know the word
- she would only be able to return by the named path if Victor were to give the name of the same path by which she had entered
- Victor would choose A or B at random, she would have a 50% chance of guessing correctly.
- If they were to repeat this trick many times:

The chance: $(1/2) * (1/2) * \ldots * (1/2) = (1/2)^n \approx 0$

Extremely Strong Authentication

Two balls and the color-blind friend



Alice is prover and not color-blind.

Bob is verifier and color-blind.

Alice wants to prove has two identical but different color balls but not want to reveal which ball is the red one and which is the green.

Alice gives the balls to Bob.

For multiple times:

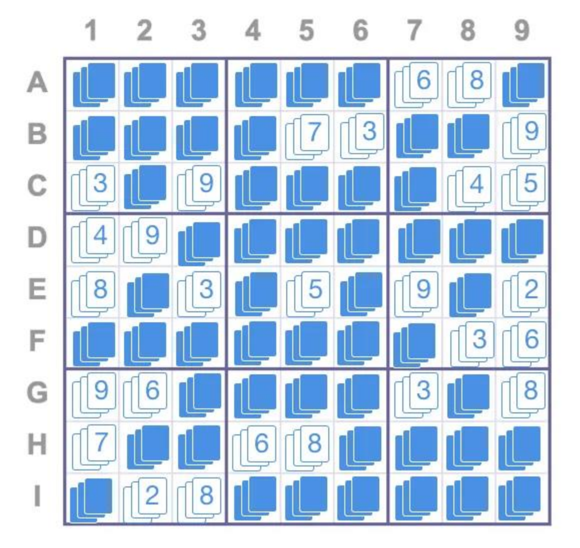
- Bob swaps the balls without Alice knowing.
- Choose one of them and shows to Alice
- Alice says it is same as the previous or is a different one

Extremely Strong Authentication

Sudoku

	1	2	3	4	5	6	7	8	9
A							6	8	
B					7	3			9
C	3		9					4	5
D	4	9							
E	8		3		5		9		2
F								3	6
G	9	6					3		8
H	7			6	8				
I		2	8						

Alice wants to prove to Bob that she has solved a Sudoku puzzle.



For each cell, Alice places 3 cards with the corresponding number. For a cell with an existing value, the cards are faced up. For the rest, they are faced down.

Bob can request each arbitrary row/column/subgroup.

The card would be shuffled before giving back to Bob.

Bob flips the cards over and verifies the numbers 1 through 9 without any numbers missing or duplicated.

Extremely Strong Authentication

Fiat-Shamir identification protocol

Theorem

$N=pq$ (p and q are large prime number)

$r^2 \mod N$

↓

Finding r is hard-problem

Extremely Strong Authentication

Fiat–Shamir identification protocol

secret S
private r
public N
public $x=r^2 \bmod N$
public $v=S^2 \bmod N$

commitment
$x=r^2 \bmod N$ →

challenge
$e=0$ or $e=1$ ←

response
$y=rS^e \bmod N$ →

Verification:

$$y^2 \overset{?}{=} xv^e \bmod N$$

Extremely Strong Authentication

Fiat-Shamir identification protocol

secret S 101
private r 42
public N 7*11=77
public $x=r^2$ mod N 70
public $v=S^2$ mod N 37

commitment
$x=r^2$ mod N 70

challenge
e=0 or e=1

response
$y=rS^e$ mod N 42 or 7

Verification:

$y^2 \stackrel{?}{=} xv^e \bmod N$
70 = 70 * 1
49 = 70 * 37

Extremely Strong Authentication

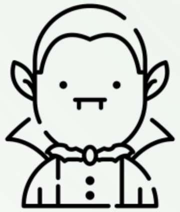
Fiat-Shamir identification protocol

Trudy guesses Bob sends $e=0$

$x=r^2 \bmod N$ →

$e=0$ ←

$y=r \bmod N$ →



Trudy guesses Bob sends $e=1$

$x=r^2v^{-1} \bmod N$ →

$e=1$ ←

$y=r \bmod N$ →

- Because Trudy does not know challenge `e`, his chance is almost zero like Alibaba cave.
- If Trudy can find `r` in $r^2 \bmod N$, he can easily find the secret `S`!

Extremely Strong Authentication

Feige-Fiat-Shamir identification protocol

n secrets

$S_1, S_2, \ldots, S_n$

private r

public N

public $x = r^2 \bmod N$

public $v_i = S_i^2 \bmod N$

commitment

$x = r^2 \bmod N$

challenge

$e_1, e_2, \ldots, e_n$

response

$y = r S_1^{e1} S_2^{e2} \ldots S_n^{en} \bmod N$

Verification:

$y^2 \stackrel{?}{=} x v_1^{e1} v_2^{e2} \ldots v_n^{en} \bmod N$

Extremely Strong Authentication

Discrete Logarithm Problem (DLP)

Theorem

a finite cyclic group G

with a generator g

with a large prime modulo p

$x = g^h \mod p$

↓

For a given x, Finding h is hard-problem

Extremely Strong Authentication

Some Terms: generator

is an element that generates the entire group when raised to different powers.

Example:

- a multiplicative group Z^*_7
- elements of the group: {1,2,3,4,5,6}
- '3' is a generator

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

$3^4 \bmod 7 = 4$

$3^5 \bmod 7 = 5$

$3^6 \bmod 7 = 1$

Extremely Strong Authentication

Some Terms: order of element

refers to the smallest positive integer n such that raising the element g to the power of n yields the identity element of the group. (`ord(g) = n`)

Example:

- a multiplicative group Z^*_{11}
- elements of the group: {1,2,3,4,5,6,7,8,9,10}
- ord(3) = 5

$3^1 \bmod 11 = 3$

$3^2 \bmod 11 = 9$

$3^3 \bmod 11 = 5$

$3^4 \bmod 11 = 4$

$3^5 \bmod 11 = 1$

Extremely Strong Authentication

Some Terms: order of group

The number of elements contains

Example:

- a multiplicative group Z^*_{11}
- elements of the group: {1,2,3,4,5,6,7,8,9,10}
- order: 10

The presentation avoids using too many mathematical concepts.

Me

Extremely Strong Authentication

Schnorr

setup:
Public key $A=g^a \mod p$
Private key a is random from range $[0,q-1]$
$q \mid p-1$

agreement on:
cyclic group G of prime order q, with a generator g

Private random v from range $[0,q-1]$

commitment
$c=g^v \mod p$

challenge
e from range $[0,2^t-1]$

response
$y=v+a*e \mod q$

agreement on:
cyclic group G of prime order q, with a generator g

Verification:

$$g^y \stackrel{?}{=} c * A^e \mod p$$

Ref

1. Cryptography Protocols Course, Dr. Hamid Mala, University of Isfahan
2. https://datatracker.ietf.org/doc/html/rfc8235
3. https://blog.goodaudience.com/understanding-zero-knowledge-proofs-through-simple-examples-df673f796d99
4. https://en.wikipedia.org/wiki/Zero-knowledge_proof#Definition
5. https://www.iconfinder.com/UsersInsights
6. https://www.iconfinder.com/Chanut-is

7eRoM