Privacy and Security of Data

[privacy protecting – zero knowledge protocols]

MoshAhmed@gmail.com

2018-08-08

Consumer Privacy Issues

- Cookies, behavioural targeting and malware
- Consumer privacy issues on social media

Protocol 1

Example

- Alan: Do you know Eve's phone?
- Bob: Yes.
- Alan: Prove it.
- Bob: 650-555-1234

Is this a good protocol?

Protocol 2

Example

- Alan: Do you know Eve's phone?
- Bob: Yes.
- Alan: Prove it.
- Bob: 650-…

Is this a good protocol?

Protocol 3

Example

- Alan: Do you know Eve’s phone?
- Bob: Yes.
- Alan: Prove it, what is last digit?
- Bob: 4

Is this a good protocol?

Protocol 4

Example

- Alan: Do you know Eve’s phone?
- Bob: Yes.
- Alan: Prove it, what is the sum of digits?
- Bob: 36

Is this a good protocol?

One Way Function

Hashing/fingerprinting, given the knowledge (account number) you can compute the sum (fingerprint) but you can't get the account number from the sum.

Protocol 5 – one way hashing

Example

- Alan: Do you know Eve’s phone?
- Bob: Yes.
- Alan: Prove it, what is the sha2 hash digits?
- Bob: 2dd619305603f60f68bc…

Is this a good protocol?

Protocol 6 – hash + challenge response

Example

- Alan: Do you know Eve's phone?
- Bob: Yes.
- Alan: Prove it, what is the first 3 hex digits of the sha2 hash digits?
- Bob: 0x2dd

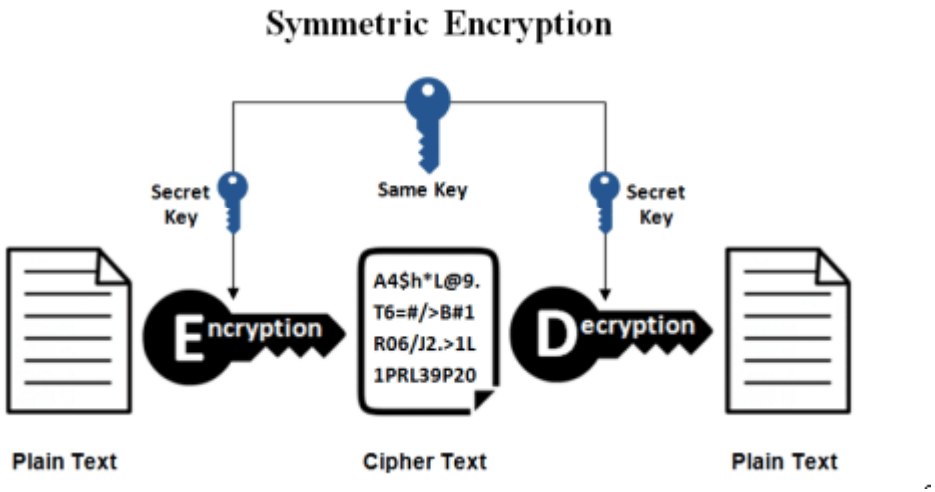
Is this a good protocol?

Zero knowledge proofs

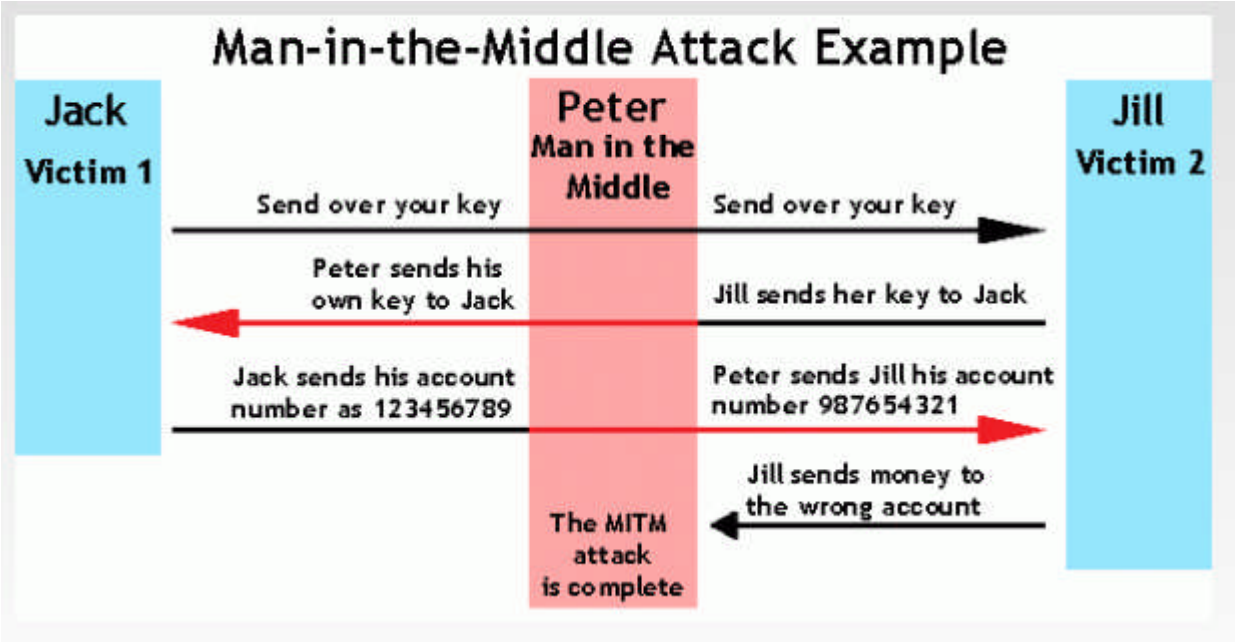
Zero-knowledge proof or **Zero-knowledge protocol** is a method by which one party (the *prover*) can prove to another party (the *verifier*) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true

How to transmit knowledge when others are listening

Solution 1 – communication over insecure channel



Problem – how to exchange keys?



Solution 2 – communication over insecure channel

Send a box of chocolate via rogue courier?

A. Sends locked box with chocolate

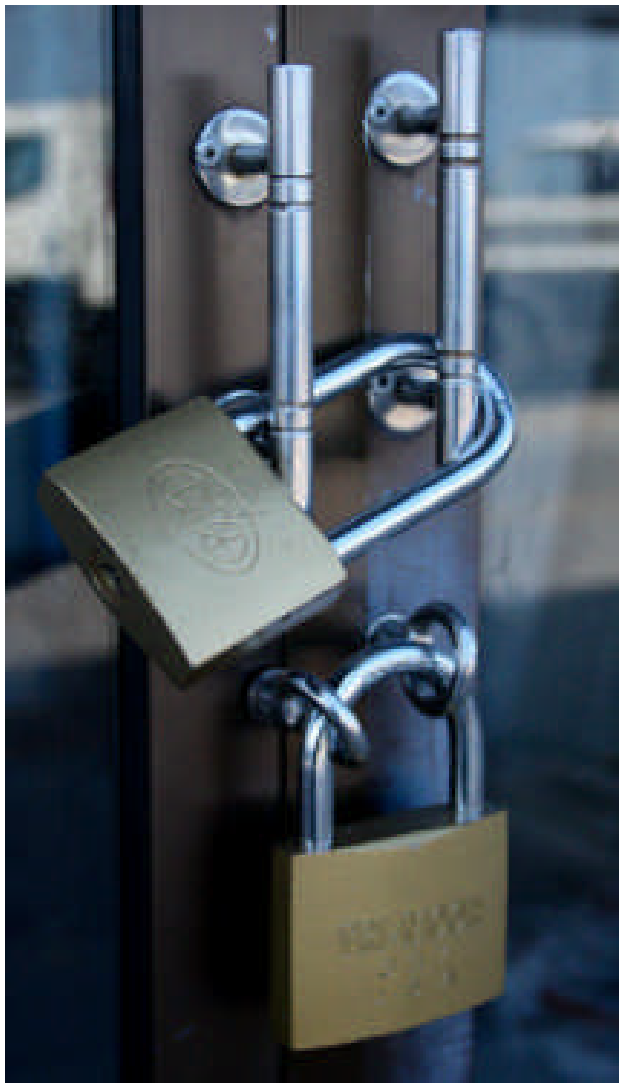
B. Puts his own lock and send back to A.

A. Removes his own lock and sends it to B with B's lock.

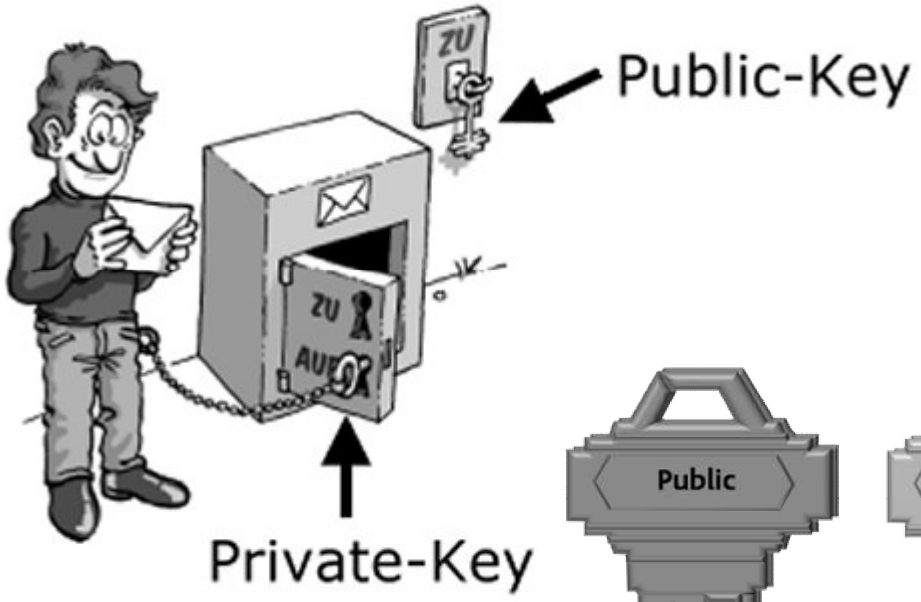
Is this solution good?

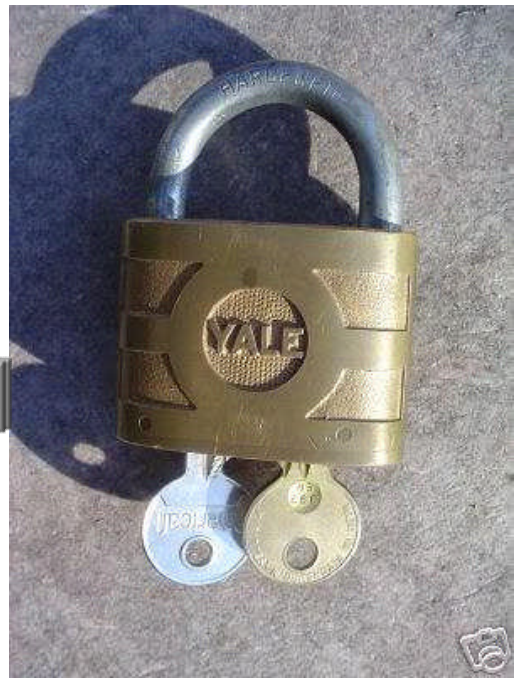
Or-Locks [Series]
(opens with any one key)

And-Locks [Parallel]
(open needs all keys)



Lock analogy for PK





Application - SSH

- You never send your private key to login server
- Server sends a challenge - a random number encrypted with your public key
- Only you can open it and send the answer back to the server and prove you have the private key.
- Server lets you login.

Problem: How do you find out the Average salary with no one revealing their own salary?

Solution

- Everyone adds their own secret random number to their information.
- All the numbers are added up in some order.
- Everyone subtracts their own random number from the total in different order.
- Divide the total by number of participants.
- Assume no one is giving wrong information.

Applications

- Banking
- Block chain
- Voting (audit trail, anonymity)
- Data analysis
- AI and machine learning.

References

- Reference https://en.wikipedia.org/wiki/Zero-knowledge_proof
- Wikipedia RSA, Public Key, Key Exchange, Diffie Hellman.
- https://www.schneier.com/books/applied_cryptography/ Classic book, chapters 1-2 on Protocols.