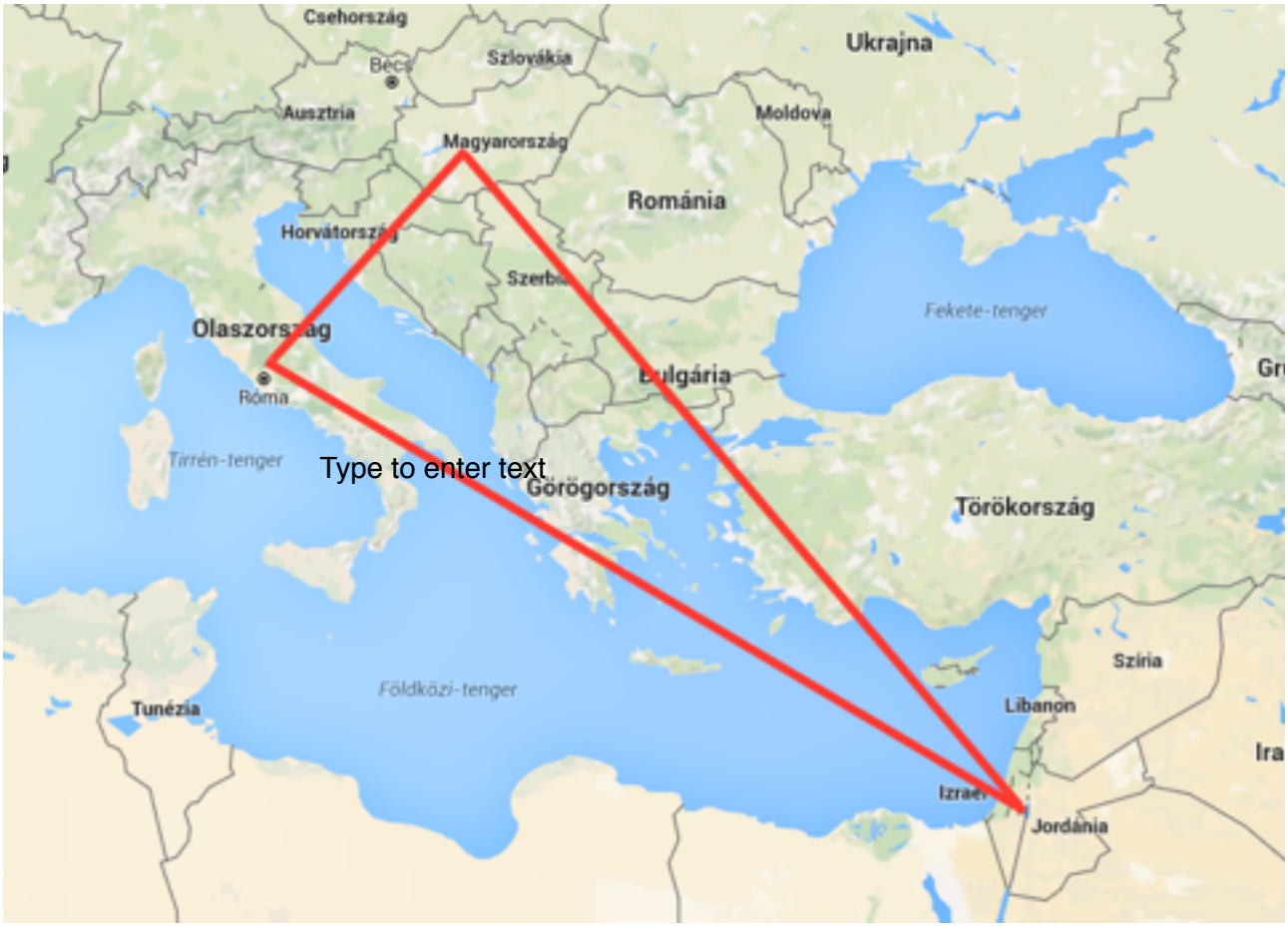
Linkek:
https://en.wikipedia.org/wiki/Zero-knowledge_proof
http://index.hu/tech/2014/02/05/johet_a_feltorhetetlen_titkositas/
http://www.wired.com/2014/02/cryptography-breakthrough/
http://www.inf.unideb.hu/~pethoe/Jegyzet_PA_20110508.pdf /175 oldal
https://en.wikipedia.org/wiki/Feige%E2%80%93Fiat%E2%80%93Shamir_identification_scheme
https://en.wikipedia.org/wiki/Amos_Fiat



https://en.wikipedia.org/wiki/Uriel_Feige
https://en.wikipedia.org/wiki/Adi_Shamir

http://www.tml.tkk.fi/Opinnot/Tik-110.501/1995/zeroknowledge.html#intro

https://lucatrevisan.wordpress.com/2009/05/11/cs276-lecture-24/
http://www.renyi.hu/~csirmaz/zk.html

http://www.tankonyvtar.hu/hu/tartalom/tamop425/0008_szalkai_dosa_szamelmelet/Szalkai_Dosa_Alg_szamelm.pdf

Kutatók:

- Shafi Goldwasser
- Silvio Micali
- Charles Rackoff
- László Babai
- Shlomo Moran
- Dwork Naor
- Amit Sahai
- Manuel Blum
- Paul Feldman

Fogalmak:

- interactive proof
- Zero-knowledge proof
- PP complex
- NP, CO-NP complex
- Zero-knowledge password proof
- Non-interactive zero-knowledge proof
- soundness
- completeness
- zero-knowledge
- lattice problem

Példák:

- barlangos
- prímes
- hamilton körös

Történet:

- 1985: Shafi, Silvio, Charles
- 1988: Blum, Feldman, Micali
- 1993: Gödel prize
- 2004: Dwork, Naor, Sahai
- 2013:

Felhasználás:

- titkosítás
- visszafejthetetlen program