Zero-Knowledge Proofs

Peggy has a secret (password, PIN, ...).

Prover

Verifier

Can Peggy convince Victor that she knows the secret, without showing it to Victor?

We will show that this is possible.

Assumption 1: Given a large graph G that contains a Hamilton cycle, it is not possible to compute such a cycle in a reasonable amount of time.

It is easy to construct a large graph that contains a Hamilton cycle:

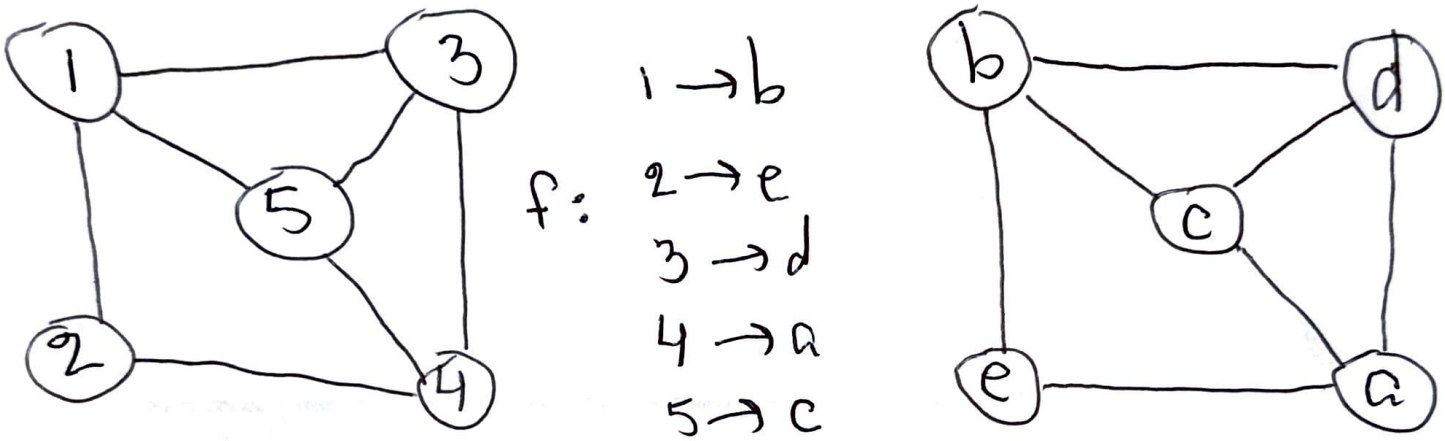
* vertex set $V = \{1, 2, \ldots, n\}$
* take a permutation $(A_1, A_2, \ldots, A_n)$ of V
* include the edges $\{A_1, A_2\}, \{A_2, A_3\}, \ldots, \{A_{n-1}, A_n\}, \{A_n, A_1\}$
* add some more edges

---

graphs $G = (V, E)$ and $G' = (V', E')$ are isomorphic if there is a bijection $f: V \to V'$ such that for all $u, v \in V$, $u \neq v$:

$$\{u, v\} \in E \iff \{f(u), f(v)\} \in E'.$$

in English: G and G′ are the same graphs, except that their vertices have different names.



Assumption 2: Given two isomorphic graphs G and G′, it is not possible to compute the bijection f in a reasonable amount of time.

Given $G = (V, E)$, it is easy to compute a graph $G' = (V, E')$ that is isomorphic to G:

* $V = \{1, 2, \ldots, n\}$
* take a permutation $(A_1, A_2, \ldots, A_n)$ of V
* for each edge $\{i, j\}$ in E:

  add $\{A_i, A_j\}$ to E'.

Peggy constructs a large graph G that contains a Hamilton cycle HC.

Peggy's secret = HC

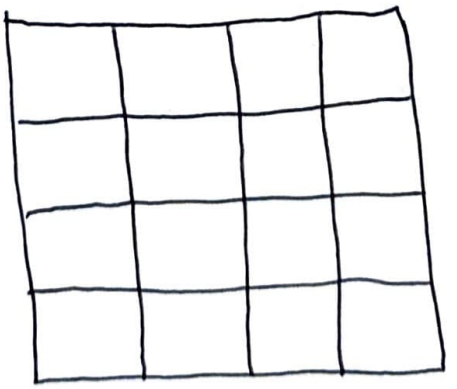
Peggy shows G to Victor.
↳ the adjacency matrix A of

Peggy's task: convince Victor that she knows HC, without showing HC to him.

Protocol:

Step 1: Peggy computes a graph G' that is isomorphic to G.

* Peggy does not show the bijection f to Victor
* Peggy shows the adjacency matrix A' of G' to Victor. However, all entries of A' are invisible to Victor.

$A' =$ 

Step 2: Victor asks Peggy exactly one of the following two questions:

Q1: Show me a Hamilton cycle in G'.

Q2: Show me that G and G' are isomorphic.

Step 3: if Victor asks Q1:

* Peggy knows Hamilton cycle HC in G, and she knows the bijection f
* Peggy computes (using f) a Hamilton cycle HC' in G'.
* Peggy makes the entries in A' that correspond to the edges in HC' visible (all other entries remain invisible).

~~shows A to Victor~~

if Victor asks Q2:

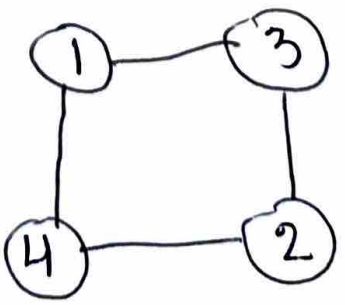
* Peggy makes <u>all</u> entries of A′ visible, and she shows Victor the bijection f.

<u>Step 4</u>: if Q1 was asked:

* Victor verifies that the visible entries in A′ corresponds to a Hamilton cycle in G′:

	1	2	3	4
1			1	
2				1
3		1		
4	1			

entry (1,3) is 1 : edge {1,3}
entry (3,2) is 1 : edge {3,2}
entry (2,4) is 1 : edge {2,4}
entry (4,1) is 1 : edge {4,1}

∴ Hamilton cycle 

in G′

if Q_2 was asked:

* Victor knows the adjacency matrix A of G, the adjacency matrix A' of G', and the bijection f
* Victor verifies that G and G' are isomorphic.

Conclusion: if Peggy knows the Hamilton cycle HC in G, she can answer Q_1 or Q_2, and Victor can verify the answer.

Since Victor asks exactly one of Q_1 and Q_2, he cannot compute the Hamilton cycle HC in G in a reasonable amount of time.

Can Peggy cheat?

* Assume Peggy does not know the Hamilton cycle HC in G.
* Victor knows the adjacency matrix A of G.

We run the protocol.

Case 1: in Step 1, Peggy computes a graph G' that is isomorphic to G, together with the bijection f. (∴ she does not cheat in Step 1.)

* if Victor asks Q1: Peggy cannot answer.
* if Victor asks Q2: Peggy can answer, and Victor can verify the answer.

* with probability $1/2$: Peggy can answer, and Victor can verify

with probability $1/2$: Victor knows that Peggy is cheating.

Case 2: Peggy cheats in Step 1: she computes a graph G' for which she knows a Hamilton cycle HC', but G' is not isomorphic to G.

* if Victor asks Q_1: Peggy can answer, and Victor can verify the answer.

* if Victor asks Q_2: Peggy cannot answer.

* with probability $1/2$: Peggy can answer, and Victor can verify
with probability $1/2$: Victor knows that Peggy is cheating.

Conclusion: With probability $1/2$, Peggy can make Victor believe that she knows the Hamilton cycle HC in G.

Exercise: * why is it important that Victor can ask only one of Q_1 and Q_2?

* why is it important that Peggy does not know which question (Q_1 or Q_2) Victor will ask?

Repeat the protocol (Steps 1-4) 100 times.

$\Pr($ Victor believes that Peggy knows the Hamilton cycle HC in G$) = (1/2)^{100}$

$\Pr($ Victor knows that Peggy is cheating$) = 1 - (1/2)^{100}$

Purpose of Q1: Victor verifies that Peggy knows Hamilton cycle in G

Purpose of Q2: Victor verifies that Peggy does not cheat in Step 1.