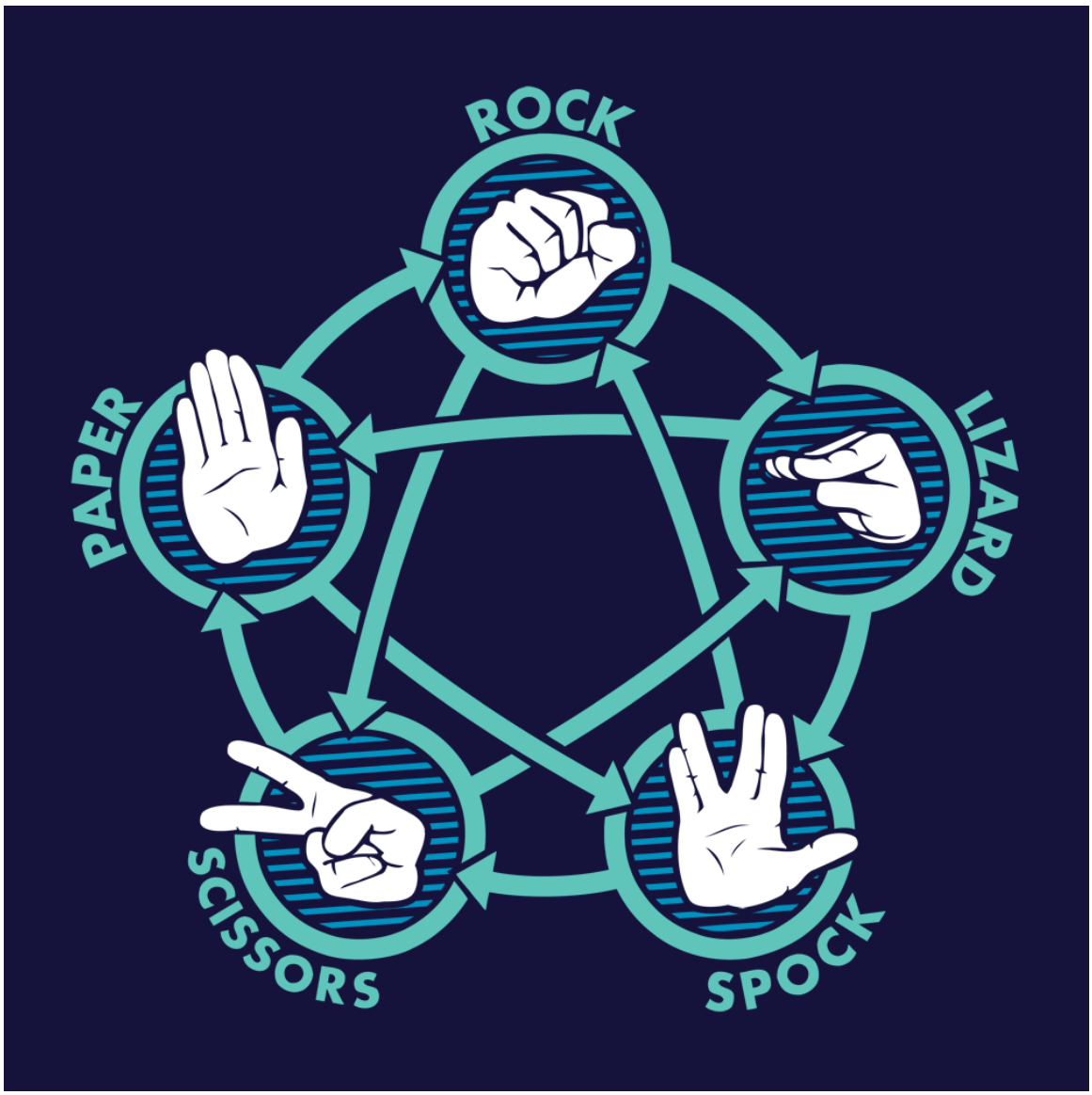
Documentation

Challenge Principles

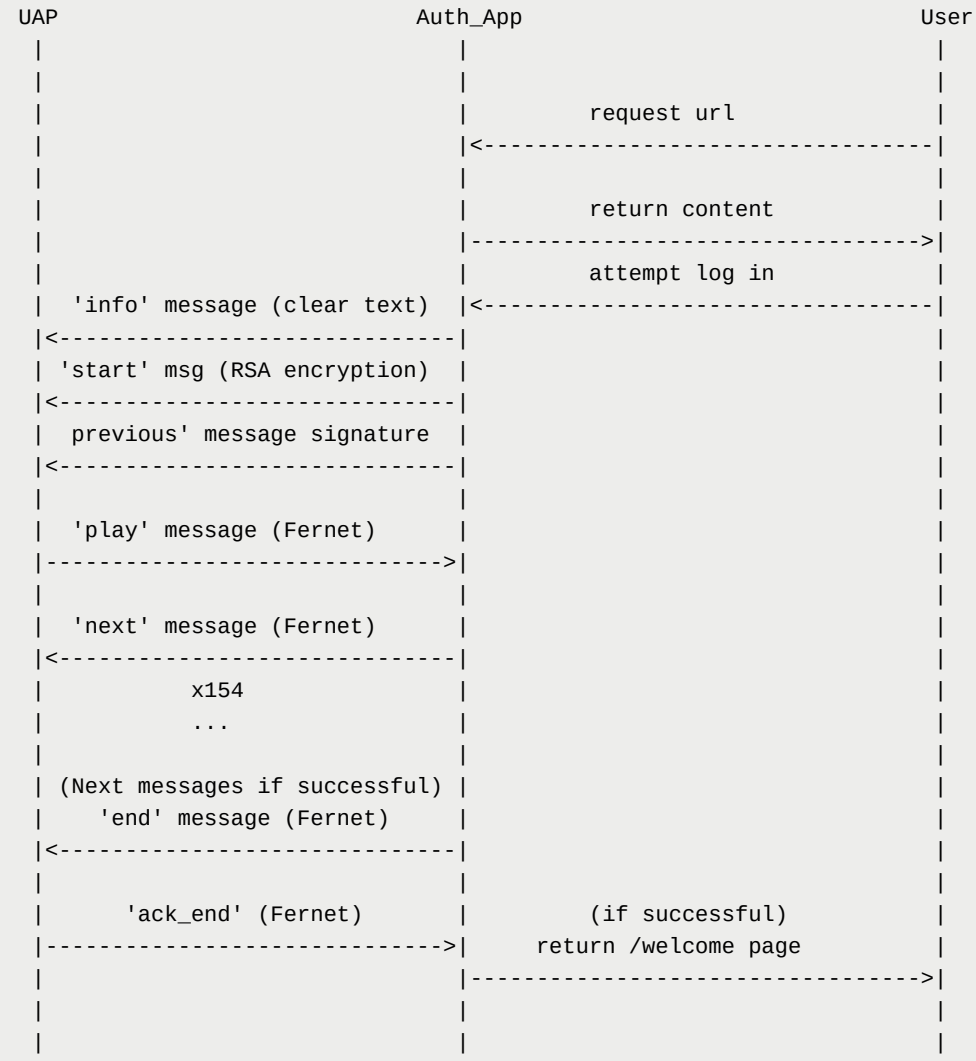
The challenge used in this protocol has of its core the game Rock, Paper, Scissors, Lizard, Spock mentioned in the famous tv series The Big Bang Theory, the game's original creator is **Steve Koenig.** The game is similar to the famous rock paper scissors game but it has some twists on it that will help later on increase the security of a game play from 1/3 to 1/5, We can see the rules by the following image:



The challenge on the authentication implemented is a game of Rock, Paper, Scissors, Lizard, Spock where the uap (user side) needs to win 154 rounds of the game against two players on the web application side. The choices of moves from the web application side will guarantee that the user has (only) one move that can win against both opponents, which gives us a 1/5 chance to pick the winning move.

The uap will play the game for 154 rounds, and the result will be announced only at the end of the full game by logging in or not, there’s no feedback given to the uap if it fails a challenge. This amount of rounds will make it so there’s a 2.28359630833e-108 chance to win the challenge if playing randomly. The web app and the uap will generate their moves with a seed derived from the user’s password, which will be a digest of the password. That digest will generate the moves for each game, and after a successful authentication the seed will be changed to its own digest, that way preventing replay attacks against the challenge. This does however require a level of synchronization between the website and the uap.

Protocol flow



- In parenthesis are the encryption used for that message
- The info message will carry just enough information to enable the uap to know which keys to decrypt/verify the next one with
- The start message contains a key to be used to encrypt all following communication.