HTTP Cookies

An HTTP "cookie" is a textual value known by both the server and client, given to the client by the server during authentication. It is later used by the client on subsequent requests to prove that the client had already authenticated before. This is a great mechanism since it allows a client to authenticate once, instead of sending the credentials on every request.
In this exercise we'll implement a similar mechanism, our own way.

Instructions

1. Continue using the same server and client as the previous exercise; rename the server to `httpcookies.py` and the client to `httpcookiesclient.py`.
2. Add support in the server for POST request to `/login` page; data (HTTP request body) should be the same as the format of the `Login-Details` header before (base64 of json with fields 'username', 'password'). If credentials are correct, server shall generate a "cookie" value (random string, 10 characters long) and send it back to client as response body (with status code 200). Server should also remember this cookie value. 2.1. Any error in login should return a 401 status code.
3. Add support in the server for `Client-Cookie` header, which should contain the cookie value. Requests to `/secret.html` should only be allowed if they contain a known cookie value. 2.2. Any rejected request to the secret page should return a 403 status code.
4. Update the client script so it first logs-in (performs authentication and gets a cookie), then requests the secret page with the cookie.

To submit

Submit server code `httpcookies.py` and client code `httpcookiesclient.py`.