■ Backend Authentication (Login & Register) - Node.js + Express

server.js

```javascript
const express = require("express");
const bcrypt = require("bcryptjs");
const jwt = require("jsonwebtoken");
const cors = require("cors");

const app = express();
const PORT = 5000;
const SECRET_KEY = "mysecretkey"; // use env variable in real projects

app.use(cors());
app.use(express.json());

// Fake DB (in-memory)
let users = [];

// Register API
app.post("/register", async (req, res) => {
  const { username, password } = req.body;

  // check if user exists
  const existingUser = users.find((u) => u.username === username);
  if (existingUser) {
    return res.status(400).json({ message: "User already exists" });
  }

  // hash password
  const hashedPassword = await bcrypt.hash(password, 10);

  // save user
  const newUser = { id: users.length + 1, username, password: hashedPassword };
  users.push(newUser);

  res.json({ message: "User registered successfully" });
});

// Login API
app.post("/login", async (req, res) => {
  const { username, password } = req.body;

  const user = users.find((u) => u.username === username);
  if (!user) {
    return res.status(400).json({ message: "User not found" });
  }

  // compare password
  const isMatch = await bcrypt.compare(password, user.password);
  if (!isMatch) {
    return res.status(400).json({ message: "Invalid credentials" });
  }

  // generate JWT token
  const token = jwt.sign({ id: user.id, username: user.username }, SECRET_KEY, {
    expiresIn: "1h",
  });

  res.json({ message: "Login successful", token });
});

// Protected API (requires token)
app.get("/profile", (req, res) => {
  const authHeader = req.headers["authorization"];
  const token = authHeader && authHeader.split(" ")[1];
  if (!token) return res.sendStatus(401);

  jwt.verify(token, SECRET_KEY, (err, user) => {
    if (err) return res.sendStatus(403);
```

```
      res.json({ message: "Welcome to your profile", user });
    });
});

app.listen(PORT, () =>
  console.log(`■ Auth API running on http://localhost:${PORT}`)
);
```

package.json

```
{
  "name": "auth-backend",
  "version": "1.0.0",
  "main": "server.js",
  "scripts": { "start": "node server.js" },
  "dependencies": {
    "bcryptjs": "^2.4.3",
    "cors": "^2.8.5",
    "express": "^4.18.2",
    "jsonwebtoken": "^9.0.0"
  }
}
```

Instructions

```
1. Create a folder `auth-backend`
2. Add `server.js` and `package.json` files with the above code
3. Run:
   npm install
   npm start

4. APIs:
   - Register: POST http://localhost:5000/register
     body: { "username": "test", "password": "1234" }
   - Login: POST http://localhost:5000/login
   - Profile (protected): GET http://localhost:5000/profile
     header: Authorization: Bearer <token>
```