**Important: private key safety pt.2**

**How to not have your private key in the command line**

Some lessons ago we deployed SimpleStorage using the following command:

forge script script/DeploySimpleStorage.s.sol --rpc-url http://127.0.0.1:8545 --broadcast --private-key 0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5efcae784d7bf4f2ff80

Having our private key in plain text is very bad, as we've explained in [Lesson 13](https://updraft.cyfrin.io/courses/foundry/foundry-simple-storage/private-key-safety). What can we do to avoid this, except using the --interactive parameter, because we don't want to keep copy-pasting our private key?

**BIG BOLDED DISCLAIMER: What we are about to do is fine for development purposes, do not put a real key here, it very terrible for production purposes.**

Create a new file in the root of your project called .env. Then, go the .gitignore file and make sure .env is in there.

The .env file will host environment variables. Variables that are of a sensitive nature that we don't want to expose in public.

Open the file and put the following in it:

PRIVATE\_KEY=0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5efcae784d7bf4f2ff80

RPC\_URL=http://127.0.0.1:8545

Next run source .env. This adds the above-mentioned environment variables into our shell. Now run echo $PRIVATE\_KEY or echo $RPC\_URL to check if the values are stored in the shell.

Now we can safely replace the parameters in our forge script command:

forge script script/DeploySimpleStorage.s.sol --rpc-url $RPC\_URL --broadcast --private-key $PRIVATE\_KEY

This doesn't only hide your private key from plain sight in the command line but also facilitates faster terminal usage, imagine you'd have to copy-paste the http://127.0.0.1:8545 RPC URL over and over again. It's cleaner this way.

But yes, now we have the private key in plain text in the .env file, that's not good.

**How to handle this problem with production code?**

Foundry has a very nice option called keystore. To read more about it type forge script --help in your terminal. Using forge script --keystore <PATH> allows you to specify a path to an encrypted store file, encrypted by a password. Thus your private key would never be available in plain text.

Let's agree to the following:

1. For testing purposes use a $PRIVATE\_KEY in an .env file as long as you don't expose that .env file anywhere.
2. Where real money is involved use the --interactive option or a [keystore file protected by a password](https://github.com/Cyfrin/foundry-full-course-f23?tab=readme-ov-file#can-you-encrypt-a-private-key---a-keystore-in-foundry-yet).

There's one more thing about storing keys in a .env file. Please take a look at the ["THE .ENV PLEDGE"](https://github.com/Cyfrin/foundry-full-course-f23/discussions/5). Read it, understand it and comment I WILL BE SAFE. Tweet it, Tiktok it, blog about it, make an Insta story about it, print it and put it on your fridge and share some copies with your neighbors. Please stay safe!