Key Negotiation of Bluetooth Attack

I used the Raspberry Pi OS kernel version v5.15.34 for the attack implementation.

The only variable which need to be changed is the `SMP_MAX_ENC_KEY_SIZE` in the `/home/pi/kernel/linux/net/bluetooth/smp.h`[1] file (line 143). The default value is 16 and it should be changed according to your needs to either 6, 7 or 15. The modified code can be seen in listing 1.

```
142 #define SMP_MIN_ENC_KEY_SIZE        7
143 #define SMP_MAX_ENC_KEY_SIZE        ~~16~~
```

Listing 1: Modification in the *smp.h* file for the KNOB attack

[1] `https://elixir.bootlin.com/linux/v5.15.34/source/net/bluetooth/smp.h`