Průzkum kódu

```
/* In this function we generate the key and set up an encryption
   engine using Crypto++ which we then hand over to Encrypt_file to actually
process the
   file in filename
        */
typedef unsigned char byte;

int Dastardly_encrypt(char *filename) {


    //Get a key, 16 byte key is long enough

    byte key[ 16 ];
    int i;
    memset( key, 0x00, 16); //Clean up our key

    //HACK: generate key one byte at a time.

    for(i=0;i<=sizeof(*key);i++){  //HACK: Use sizeof in case we decide to
change key length later
        key[i]=(byte)(std::rand() % 256);
        }

     //create the encryption object
    auto enc = new ECB_Mode<AES>::Encryption(key, sizeof(key));
     //encrypt the file
    i=Encrypt_file( enc, filename);

    return(i);
}
```

Tento kód má za úkol vygenerovat náhodný klíč a následně spustit šifrování dat. Pole obsahující klíč je nejdříve inicializováno na samé nuly. Následně má být klíč generován po bytech pomocí *for* cyklu. Tento cyklus je ovšem ohraničen `sizeof(*key)`. Místo délky pole je tedy získána velikost prvního prvku a jelikož prvky pole jsou `unsigned char` velikost je 1. Náhodně jsou tedy vygenerovány pouze první dva byty, zbytek zůstává nastaven na 0. Dále vidíme, že soubor je šifrován AES v ECB módu.

Brute force

Velikost prostoru klíčů je v tomto případě pouze dva byty je tedy jednoduché provést brute force útok. Ten lze provést různými způsoby, v rámci zadání je doporučeno využít Cryptool2, jehož součástí je i brute force analyzátor pro AES v ECB módu. Je tedy pouze nutné nastavit správně vstup v Base64 kódování a analyzátor spustit.