

```
_ZN4Util8decipherlN8CryptoPP7TwofishEEE10QByteArrayRKS3_Ph56_:\npush r15\npush r14\nmov r15, rdi\npush r13\npush r12\nmov r14, rdx\npush rbp\npush rbx\nmov r13, rcx\nsub rsp, 12C8h\nlea r12, [rsp+12F8h+var_12E8]\nlea rbx, [rsp+12F8h+decryptor]\nmov [rsp+12F8h+var_12F0], rsi\nmov rax, fs:28h\nmov [rsp+12F8h+var_40], rax\nxor eax, eax\nlea rax, [r12+10h]\nmov rdi, rbx\nmov qword ptr [rsp+12F8h+var_12E0], 0\nmov [rsp+12F8h+var_12D8], 0\nmov [rsp+12F8h+var_12E8], rax\ncall _ZN8CryptoPP8EAX_BaseC2Ev, CryptoPP::EAX_Base::~EAX_Base(void)\nlea rbp, _ZTVN8CryptoPP9EAX_FinalINS_7TwofishELb0EEEE, `vtable for CryptoPP::EAX_Final<CryptoPP::Twofish,false>`\nlea rdi, [rbx+0F0h]\nmov esi, 1\nlea rax, [rbp+10h]\nmov [rsp+12F8h+decryptor], rax\nlea rax, [rbp+180h]\nmov [rsp+12F8h+var_1250], rax\nlea rax, [rbp+20h]\nmov [rsp+12F8h+var_1248], rax\nlea rax, _ZTVN8CryptoPP21SimpleKeyingInterfaceE, `vtable for CryptoPP::SimpleKeyingInterface`\nadd rax, 10h\nmov [rsp+12F8h+var_1170], rax\ncall _ZN8CryptoPP9AlgorithmC2Eb, CryptoPP::Algorithm::Algorithm(bool)\nlea rax, _ZTVN8CryptoPP4CMACINS_7TwofishEEE, `vtable for CryptoPP::CMAC<CryptoPP::Twofish>`\nlea rdi, [rbx+128h]\nmov esi, 1\nmov [rsp+12F8h+var_1158], 0FFFFFFFFFFFFFFFh\nmov [rsp+12F8h+var_1150], 0\nmov [rsp+12F8h+var_1148], 0\nmov [rsp+12F8h+var_1140], 0\nlea rdx, [rax+10h]\nadd rax, 0E0h\nmov [rsp+12F8h+var_1168], rax\nlea rax, _ZTVN8CryptoPP21SimpleKeyingInterfaceE, `vtable for CryptoPP::SimpleKeyingInterface`\nmov [rsp+12F8h+var_1170], rdx\nadd rax, 10h\nmov [rsp+12F8h+var_1138], rax\ncall _ZN8CryptoPP9AlgorithmC2Eb, CryptoPP::Algorithm::Algorithm(bool)\nmov rax, 3FFFFFFFFFFFFFFFh\nlea rdx, [rax+130h]\nmov r8d, 16\nmov [rsp+12F8h+var_1080], rax\nmov [rsp+12F8h+var_60], rax\nlea rax, [rbx+1F0h]\nlea [rsp+12F8h+input], rdx\nrcx, r13, address of iv\nrsi, r14, address of key\nmov [rsp+12F8h+var_50], rax\nlea rax, _ZTVN8CryptoPP16BlockCipherFinalLNS_9CipherDirE0ENS_7Twofish3EncEEE, `vtable for CryptoPP::BlockCipherFinal<(CryptoPP::CipherDir)0, CryptoPP::Twofish>::Enc<`\nmov rdi, rbx\nmov [rsp+12F8h+var_1078], 28h\nmov [rsp+12F8h+var_1067], 1\nmov [rsp+12F8h+var_58], 400h\nmov [rsp+12F8h+var_67], 1\nlea rdx, [rax+10h]\nadd rax, 0C8h\nmov [rsp+12F8h+var_1130], rax\nmov [rsp+12F8h+var_1138], rdx\nmov edx, 16\ncall _ZN8CryptoPP21SimpleKeyingInterface12SetKeyWithIVePKhmS2_m, CryptoPP::SimpleKeyingInterface::SetKeyWithIV(uchar const*,ulong,uchar const*,ulong)\nmov edi, 20h, ```, unsigned_int64\ncall _Znwmm, operator new(ulong)\nxor esi, esi\nmov rdi, rax\nmov r13, rax\nlea _ZN8CryptoPP9AlgorithmC2Eb, CryptoPP::Algorithm::Algorithm(bool)\nlea rax, _ZTVN8CryptoPP18StringSinkTemplateINS7_cxx1112basic_stringcSt11char_traitscESaIcEEEEEE, `vtable for CryptoPP::StringSinkTemplate<std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>>`\nmov [r15+18h], r12\nmov edi, 230h, unsigned_int64\nlea rdx, [rax+10h]\nadd rax, 416\nmov [r13+8], rax\nmov [r13+0], rdx\ncall _Znwmm, operator new(ulong)\nmov r9d, 5\nmov r8d, 0FFFFFFFFh\nmov ecx, 10h\nmov rdx, r13\nmov rsi, rbx\nmov rdi, rax\nmov r14, rax\ncall _ZN8CryptoPP29AuthenticatedDecryptionFilterC2ERNS_28AuthenticatedSymmetricCipherEPNS_22BufferedTransformationEjJNS_21BlockPaddingSchemeDefI8BlockPaddingSchemeE, CryptoPP::AuthenticatedDecryptionFilter::AuthenticatedDecryptionFilter(CryptoPP::AuthenticatedSymmetricCipher &, CryptoPP::BufferedTransformation *,uint,int,CryptoPP::BlockPaddingSchemeDef::BlockPaddingScheme)\nmov rax, [rsp+8]\nlea rdi, [rsp+30h]\nmov r6, r14\nmov ecx, 1\nmov rsi, [rax]\nmovsd rdx, dword ptr [rsi+4]\nadd rsi, [rsi+16]\ncall _ZN8CryptoPP12StringSourceC2EPKhmbPNS_22BufferedTransformationE, CryptoPP::StringSource::StringSource(uchar const*,ulong,bool,CryptoPP::BufferedTransformation *)\nlea rax, _ZTVN8CryptoPP6FilterE, `vtable for CryptoPP::Filter`\nmov rdi, [rsp+48h]\nlea rdx, [rax+10h]\nadd rax, 188h\ntest rdi, rdi\nmov [rsp+12F8h+var_12C0], rax\nmov [rsp+12F8h+stringsource], rdx\njr short loc_34AC17F
```

```
mov rbp, rax\nlea rax, _ZTVN8CryptoPP9CMAC_BaseE, `vtable for CryptoPP::CMAC_Base`\nlea rdi, [rbx+0F8h]\nlea rdx, [rax+10h]\nadd rax, 0D8h\nmov [rsp+12F8h+var_1168], rax\nmov [rsp+12F8h+var_1170], rdx\ncall _ZN8CryptoPP8SecBlockInNS_20AllocatorWithCleanuphlh0EEEEED2Ev, CryptoPP::SecBlock<uchar,CryptoPP::AllocatorWithCleanup<uchar,false>>::~SecBlock()
```

```
mov rbp, rax\njmp short loc_34AC2BA
```

```
mov r14, rax\nmov rdi, r13, void *\ncall __ZdlPv, operator delete(void *)
```

```
mov r13, rax\njmp short loc_34AC219
```

```
mov rdi, r14, void *\ncall __ZdlPv, operator delete(void *)
```

```
mov rax, [rdi]\ncall qword ptr [rax+8]
```

```
mov edx, [rsp+12F8h+var_12E0], int\nmov rsi, [rsp+12F8h+var_12E8], char *\nmov rdi, r15, this\ncall _ZN10QByteArrayC1EPKc, QByteArray::QByteArray(char const*,int)\nlea rax, [rbp+10h]\nlea rdi, [rax+0E8h]\nadd rdi, 10h\nmov [rsp+12F8h+decryptor], rax\nlea rax, [rbp+180h]\nmov [rsp+12F8h+var_1250], rax\nlea rax, [rbp+230h]\nmov [rsp+12F8h+var_1248], rax\ncall _ZN8CryptoPP4CMACINS_7TwofishEED2Ev, CryptoPP::CMAC<CryptoPP::Twofish>::~CMAC()\nmov rdi, rbx\ncall _ZN8CryptoPP8EAX_BaseD2Ev, CryptoPP::EAX_Base::~EAX_Base()\nmov rdi, [rsp+12F8h+var_12E8], void *\ncmp rdi, r12\njz short loc_34AC1E1
```

```
call __ZdlPv, operator delete(void *)
```

```
mov rcx, [rsp+12F8h+var_40]\nxor rcx, fs:28h\nmov rax, r15\njnz short loc_34AC209
```

```
add rsp, 12C8h\npop rax\npop rbp\npop r12\npop r13\npop r14\npop r15\nretn
```

```
call __stack_chk_fail
```

```
mov rdi, rbx\ncall _ZN8CryptoPP8EAX_BaseD2Ev, CryptoPP::EAX_Base::~EAX_Base()\njmp short loc_34AC23A
```

```
mov rbp, rax\njmp short loc_34AC25A
```

```
lea rax, [rbp+10h]\nlea rdi, [rbx+0E8h]\nlea rax, [rsp+12F8h+decryptor], rax\nlea rax, [rbp+180h]\nmov [rsp+12F8h+var_1250], rax\nlea rax, [rbp+230h]\nmov rbp, r13\nmov [rsp+12F8h+var_1248], rax\ncall _ZN8CryptoPP4CMACINS_7TwofishEED2Ev, CryptoPP::CMAC<CryptoPP::Twofish>::~CMAC()\nmov rdi, rbx\ncall _ZN8CryptoPP8EAX_BaseD2Ev, CryptoPP::EAX_Base::~EAX_Base()
```

```
mov rdi, [rsp+12F8h+var_12E8], void *\nadd r12, 10h\ncmp rdi, r12\njz short loc_34AC26D
```

```
call __ZdlPv, operator delete(void *)
```

```
mov rdi, rbp, struct_Unwind_Exception *\ncall __Unwind_Resume
```