KU LEUVEN

Help choosing the next crypto-standard

ES&S MOL: ay 2021-2022

- ES&S
- Introduction
- Library exercise
- Experiment
- Your turn !

Embedded Systems & Security

- Research group connected to Electronics/ICT & COSIC
- Headed by prof. Nele Mentens
- Current research team:
  - 4 PhD students
  - 1 post-doc
  - 1 research expert

- ES&S
- Introduction
- Library exercise
- Experiment
- Your turn !

Introduction

Q1

What **did** you find out about this "formula" ?

cryptology = cryptography + cryptanalysis

Introduction

Q2

What is the difference between Symmetric key and Public key cryptography ?

Introduction

Q3

What is a cryptographic algorithm ?

Introduction

Q3

What is a cryptographic algorithm ?

Symmetric-key cryptography

-
-
-

Public-key cryptography

-
-
-

Introduction

Q4

Why would you optimise some code or a design towards binary size, **anno 2021** ?

Introduction Q5

How do you compile a static library in C, and how do you link with it ?

- what is the difference between a static and a dynamic library ?

- ES&S
- Introduction
- Library exercise
- Experiment
- Your turn !

demo_v1.c

```c
#include <stdio.h>

int sum(int x, int y) {
  return (int)(x+y);
}

int main(void) {
  int a, b, c;

  a = 3;
  b = 2;

  c = sum(a, b);

  printf("The sum of a + b = %d + %d = %d\n", a, b, c);

  return 0;
}
```

demo_v1.c

```c
#include <stdio.h>

int sum(int x, int y) {
  return (int)(x+y);
}

int main(void) {
  int a, b, c;

  a = 3;
  b = 2;

  c = sum(a, b);

  printf("The sum of a + b = %d + %d = %d\n", a, b, c);

  return 0;
}
```

main( )

sum( )

demo_v1.c

```c
#include <stdio.h>

int sum(int x, int y) {
  return (int)(x+y);
}

int main(void) {
  int a, b, c;

  a = 3;
  b = 2;

  c = sum(a, b);

  printf("The sum of a + b = %d + %d = %d\n", a, b, c);

  return 0;
}
```

All code in a **single** file

gcc -c demo_v1.c

gcc -o demo_v1 demo_v1.o

C source
object file
binary
static library

demo_v2.c

```c
#include <stdio.h>

#include "demo_v2_lib.h"

int main(void) {
  int a, b, c;

  a = 3;
  b = 2;

  c = sum(a, b);

  printf("The sum of a + b = %d + %d = %d\n", a, b, c);

  return 0;
}
```

demo_v2_lib.c

```c
#include "demo_v2_lib.h"

int sum(int x, int y) {
  return (int)(x+y);
}
```

demo_v2_lib.h

```c
#include <stdio.h>

int sum(int x, int y);
```

demo_v2.c

```c
#include <stdio.h>

#include "demo_v2_lib.h"

int main(void) {
  int a, b, c;

  a = 3;
  b = 2;

  c = sum(a, b);

  printf("The sum of a + b = %d + %d = %d\n", a, b, c);

  return 0;
}
```

demo_v2_lib.c

```c
#include "demo_v2_lib.h"

int sum(int x, int y) {
  return (int)(x+y);
}
```

demo_v2_lib.h

```c
#include <stdio.h>

int sum(int x, int y);
```

demo_v2.c

```c
#include <stdio.h>

#include "demo_v2_lib.h"

int main(void) {
  int a, b, c;

  a = 3;
  b = 2;

  c = sum(a, b);

  printf("The sum of a + b = %d + %d = %d\n", a, b, c);

  return 0;
}
```

demo_v2_lib.c

```c
#include "demo_v2_lib.h"

int sum(int x, int y) {
  return (int)(x+y);
}
```

demo_v2_lib.h

```c
#include <stdio.h>

int sum(int x, int y);
```

All code in **separate** files

gcc -c demo_v2_lib.c

gcc -c demo_v2.c

gcc -o demo_v2 demo_v2.o demo_v2_lib.o

C source
object file
binary
static library

code is unaltered !!

demo_v2.c

```c
#include <stdio.h>

#include "demo_v2_lib.h"

int main(void) {
  int a, b, c;

  a = 3;
  b = 2;

  c = sum(a, b);

  printf("The sum of a + b = %d + %d = %d\n", a, b, c);

  return 0;
}
```

demo_v2_lib.c

```c
#include "demo_v2_lib.h"

int sum(int x, int y) {
  return (int)(x+y);
}
```

demo_v2_lib.h

```c
#include <stdio.h>

int sum(int x, int y);
```

code is unaltered !!

demo_v2.c

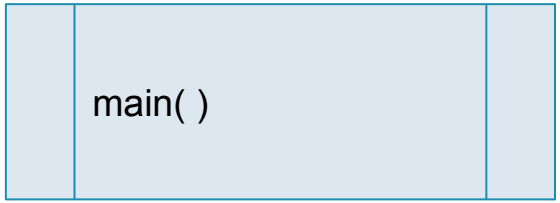
```c
#include <stdio.h>

#include "demo_v2_lib.h"

int main(void) {
  int a, b, c;

  a = 3;
  b = 2;

  c = sum(a, b);

  printf("The sum of a + b = %d + %d = %d\n", a, b, c);

  return 0;
}
```

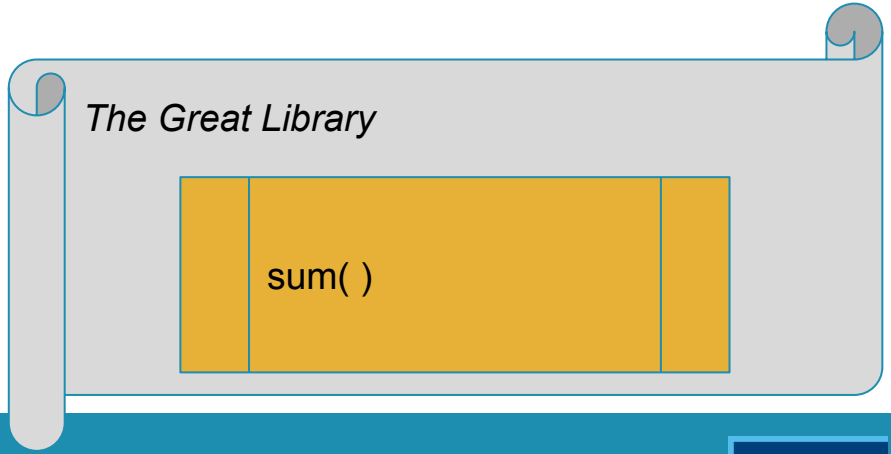
demo_v2_lib.c

```c
#include "demo_v2_lib.h"

int sum(int x, int y) {
  return (int)(x+y);
}
```

demo_v2_lib.h

```c
#include <stdio.h>

int sum(int x, int y);
```





code is unaltered !!

demo_v2.c

```c
#include <stdio.h>

#include "demo_v2_lib.h"

int main(void) {
  int a, b, c;

  a = 3;
  b = 2;

  c = sum(a, b);

  printf("The sum of a + b = %d + %d = %d\n", a, b, c);

  return 0;
}
```

demo_v2_lib.c

```c
#include "demo_v2_lib.h"

int sum(int x, int y) {
  return (int)(x+y);
}
```

demo_v2_lib.h

```c
#include <stdio.h>

int sum(int x, int y);
```

gcc -c demo_v2_lib.c

ar -rcs libdemo_v2.a demo_v2_lib.o

gcc -c demo_v3.c

gcc -o demo_v3 demo_v3.o *-L.* -ldemo_v2

C source

object file

binary

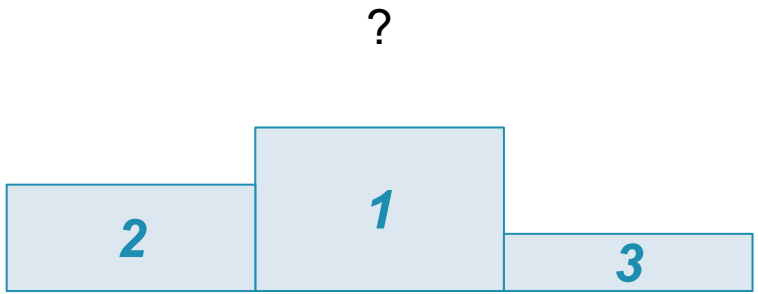
static library

- ES&S
- Introduction
- Library exercise
- <u>Experiment</u>
- Your turn !

Setting

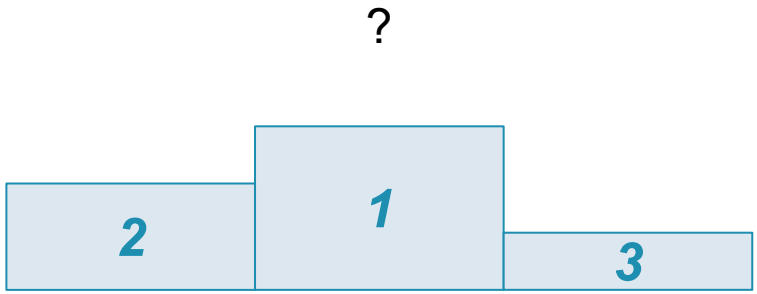
- Ongoing competition: https://csrc.nist.gov/projects/lightweight-cryptography/

- 10 finalists



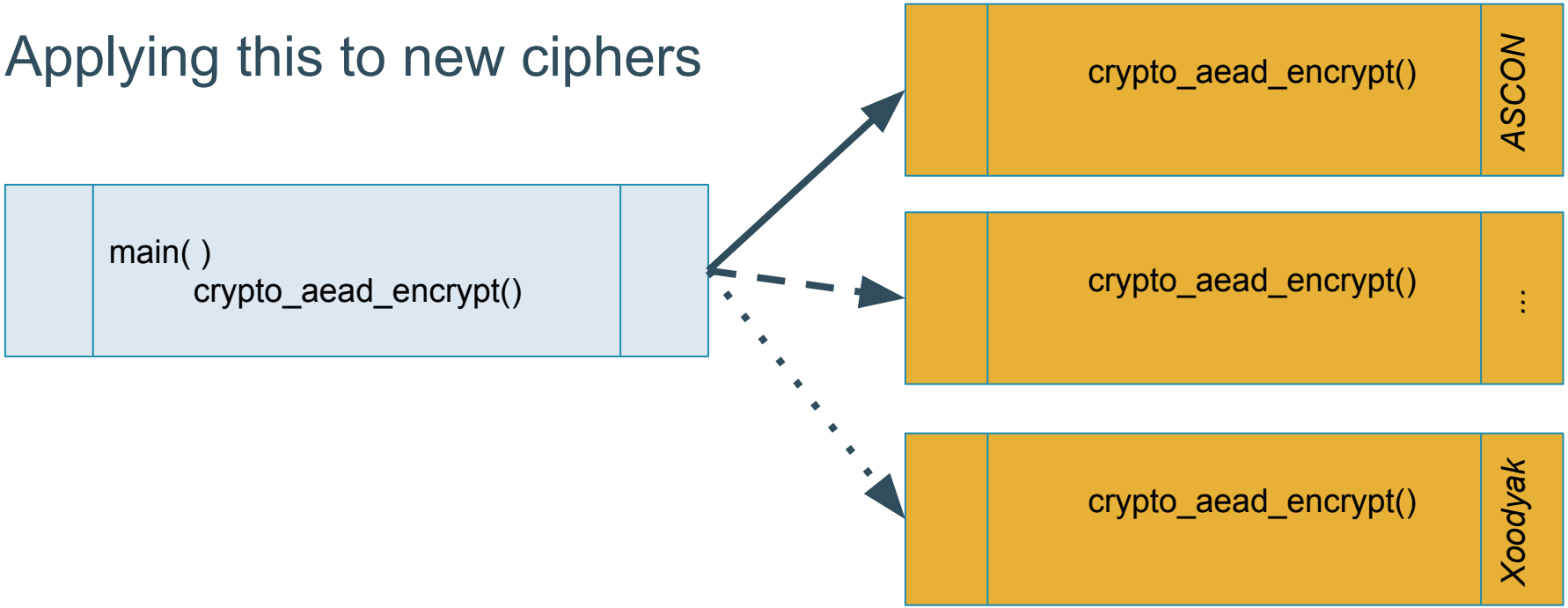
Setting

- speed
- file size
- optimal input size
- ...



A little help

Applying this to new ciphers



- ES&S
- Introduction
- Library exercise
- Experiment
- Your turn !

Labsetup

- WiFi: ES&S_2.4_lab - 35&5_l@b/

Server IP address: 192.168.1.10

User profiles: guest*n* met *n* {1, 2, 3, 4, 5},

Vb: user: “guest2”, ww: “guest2”