

OTPNitro

Generated by Doxygen 1.8.3.1

Fri Jun 27 2014 19:48:41



# Contents

- 1 Class Index** **1**
- 1.1 Class List 1
  
- 2 File Index** **3**
- 2.1 File List 3
  
- 3 Class Documentation** **5**
- 3.1 Config Class Reference 5
- 3.1.1 Detailed Description 5
- 3.1.2 Constructor & Destructor Documentation 5
- 3.1.2.1 Config 5
- 3.1.3 Member Function Documentation 6
- 3.1.3.1 getChars 6
- 3.1.3.2 getPages 6
- 3.1.3.3 getPath 6
- 3.1.3.4 saveConfig 6
- 3.1.3.5 setChars 6
- 3.1.3.6 setPages 6
- 3.1.3.7 setPath 7
- 3.2 Crypto Class Reference 7
- 3.2.1 Detailed Description 7
- 3.2.2 Member Function Documentation 7
- 3.2.2.1 decrypt 7
- 3.2.2.2 encrypt 7
- 3.3 Page Class Reference 8
- 3.3.1 Detailed Description 8
- 3.3.2 Constructor & Destructor Documentation 8
- 3.3.2.1 Page 8
- 3.3.3 Member Function Documentation 9
- 3.3.3.1 burn 9
- 3.3.3.2 generate 9
- 3.3.3.3 get 9

---

3.3.3.4	list	9
3.3.3.5	next	9
3.3.3.6	read	10
3.3.3.7	write	10
3.4	Rand Class Reference	10
3.4.1	Detailed Description	10
3.4.2	Constructor & Destructor Documentation	11
3.4.2.1	Rand	11
3.4.3	Member Function Documentation	11
3.4.3.1	genSeed	11
3.4.3.2	getChar	11
3.4.3.3	getLetter	11
3.4.3.4	getNumber	11
3.4.3.5	getSeed	12
3.4.3.6	getTicks	12
3.4.3.7	setSeed	12
3.5	Text Class Reference	12
3.5.1	Detailed Description	13
3.5.2	Member Function Documentation	13
3.5.2.1	create	13
3.5.2.2	decodeB26	13
3.5.2.3	encodeB26	13
3.5.2.4	parse	13
3.5.2.5	print	14
3.5.2.6	replaceAll	14
3.5.3	Member Data Documentation	14
3.5.3.1	book	14
3.5.3.2	from	14
3.5.3.3	msg	14
3.5.3.4	page	14
<b>4</b>	<b>File Documentation</b>	<b>15</b>
4.1	base24.cpp File Reference	15
4.1.1	Function Documentation	15
4.1.1.1	main	15
4.2	base24.h File Reference	16
4.3	config.cpp File Reference	16
4.4	config.h File Reference	16
4.5	crypto.cpp File Reference	17
4.6	crypto.h File Reference	18

---

---

4.7	otpnitro.cpp File Reference	19
4.7.1	Function Documentation	20
4.7.1.1	main	20
4.8	otpnitro.h File Reference	20
4.8.1	Macro Definition Documentation	20
4.8.1.1	MAX_PATH	20
4.8.1.2	SPACING	20
4.8.1.3	VERSION	20
4.9	page.cpp File Reference	20
4.10	page.h File Reference	21
4.11	prngtest.cpp File Reference	22
4.11.1	Macro Definition Documentation	23
4.11.1.1	LOOPCNT	23
4.11.2	Function Documentation	23
4.11.2.1	main	23
4.12	rand.cpp File Reference	23
4.13	rand.h File Reference	23
4.14	text.cpp File Reference	24
4.15	text.h File Reference	25
	<b>Index</b>	<b>26</b>



# Chapter 1

## Class Index

### 1.1 Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

<a href="#">Config</a>	Configuration, path and pages management . . . . .	5
<a href="#">Crypto</a>	Crypt and decrypt class . . . . .	7
<a href="#">Page</a>	<a href="#">Page</a> operations class . . . . .	8
<a href="#">Rand</a>	This class provides all secure random routines . . . . .	10
<a href="#">Text</a>	<a href="#">Text</a> and encoding related functions . . . . .	12





# Chapter 2

## File Index

### 2.1 File List

Here is a list of all files with brief descriptions:

<a href="#">base24.cpp</a>	15
<a href="#">base24.h</a>	16
<a href="#">config.cpp</a>	16
<a href="#">config.h</a>	16
<a href="#">crypto.cpp</a>	17
<a href="#">crypto.h</a>	18
<a href="#">otpnitro.cpp</a>	19
<a href="#">otpnitro.h</a>	20
<a href="#">page.cpp</a>	20
<a href="#">page.h</a>	21
<a href="#">prngtest.cpp</a>	22
<a href="#">rand.cpp</a>	23
<a href="#">rand.h</a>	23
<a href="#">text.cpp</a>	24
<a href="#">text.h</a>	25



# Chapter 3

## Class Documentation

### 3.1 Config Class Reference

Configuration, path and pages management.

```
#include <config.h>
```

#### Public Member Functions

- [Config](#) (void)  
*Config constructor.*
- int [getChars](#) ()  
*Returns the max PATH length.*
- int [getPages](#) ()  
*Returns the number of generated pages.*
- char \* [getPath](#) ()  
*Returns the current PATH.*
- void [setChars](#) (int)  
*Set the max PATH length.*
- void [setPages](#) (int)  
*Set the num of pages to be generated.*
- void [setPath](#) (char \*)  
*Set a new PATH to be used.*
- void [saveConfig](#) ()  
*Save the config to the default PATH  
If the config file doesnt exist it will create it with default values.*

#### 3.1.1 Detailed Description

Configuration, path and pages management.

#### 3.1.2 Constructor & Destructor Documentation

##### 3.1.2.1 Config::Config ( void )

[Config](#) constructor.

**Returns**

[Config](#) object

**Default PATH**

Win32: The PATH is %APPDATA%\otpnitro\

Unix: The PATH is \$HOME/.otpnitro/

**Files**

The config file is always otpnitro.ini in the PATH root.

The pages are stored on the PAGES folder from the PATH root.

**3.1.3 Member Function Documentation****3.1.3.1 int Config::getChars ( )**

Returns the max PATH length.

**Returns**

MAX\_CHARS

**3.1.3.2 int Config::getPages ( )**

Returns the number of generated pages.

**Returns**

MAX\_PAGES

**3.1.3.3 char \* Config::getPath ( )**

Returns the current PATH.

**3.1.3.4 void Config::saveConfig ( void )**

Save the config to the default PATH

If the config file doesnt exist it will create it with default values.

**3.1.3.5 void Config::setChars ( int *chars* )**

Set the max PATH length.

**Parameters**

<i>chars</i>	MAX_CHARS (int)
--------------	-----------------

**3.1.3.6 void Config::setPages ( int *pages* )**

Set the num of pages to be generated.

## Parameters

<i>pages</i>	MAX_PAGES (int)
--------------	-----------------

## 3.1.3.7 void Config::setPath ( char \* path )

Set a new PATH to be used.

The documentation for this class was generated from the following files:

- [config.h](#)
- [config.cpp](#)

## 3.2 Crypto Class Reference

Crypt and decrypt class.

```
#include <crypto.h>
```

### Public Member Functions

- string [decrypt](#) (string, string)  
*Decrypt a text (crypted) string.*
- string [encrypt](#) (string, string)  
*Crypt a text string.*

### 3.2.1 Detailed Description

Crypt and decrypt class.

### 3.2.2 Member Function Documentation

#### 3.2.2.1 string Crypto::decrypt ( string crypted, string out )

Decrypt a text (crypted) string.

## Parameters

<i>crypted</i>	Original (crypted) string
<i>out</i>	The ciphered text to sum(26)

## Returns

The decrypted string

This function also replaces all "JQ" occurrences from the decrypted text to spaces

#### 3.2.2.2 string Crypto::encrypt ( string in, string out )

Crypt a text string.

**Parameters**

<i>in</i>	Original (not crypted) string
<i>out</i>	The ciphered text to sum(26)

**Returns**

The crypted string

This function also remove the newline chars and replace all spaces to the "JQ" from the original text before to be crypted

The documentation for this class was generated from the following files:

- [crypto.h](#)
- [crypto.cpp](#)

### 3.3 Page Class Reference

[Page](#) operations class.

```
#include <page.h>
```

**Public Member Functions**

- [Page](#) (void)  
*The constructor sets all parameters from the [Config](#) object.*
- bool [generate](#) (string)  
*Generate a complete Book using [Page::get\(\)](#) and write it to the disk.*
- bool [write](#) (int, string, string)
- int [next](#) (string)  
*Returns the next unused page num for a book.*
- bool [burn](#) (int, string)  
*Secure page file delete.*
- string [read](#) (int, string)  
*Get the ciphertext page from a given book.*
- string [get](#) ()  
*Generate ciphertext page using the [Rand](#) class.*
- string [list](#) ()  
*Returns a list of valid books.*

#### 3.3.1 Detailed Description

[Page](#) operations class.

#### 3.3.2 Constructor & Destructor Documentation

##### 3.3.2.1 [Page::Page](#) ( void )

The constructor sets all parameters from the [Config](#) object.

**Returns**

[Page](#) object

### 3.3.3 Member Function Documentation

#### 3.3.3.1 `bool Page::burn ( int page, string id )`

Secure page file delete.

##### Parameters

<i>page</i>	Page num
<i>id</i>	Book ID

##### Returns

(bool) true == ok

#### 3.3.3.2 `bool Page::generate ( string id )`

Generate a complete Book using [Page::get\(\)](#) and write it to the disk.

##### Parameters

<i>id</i>	New book ID
-----------	-------------

##### Returns

(bool) true == ok

#### 3.3.3.3 `string Page::get ( )`

Generate ciphertext page using the [Rand](#) class.

##### Returns

ciphertext

#### 3.3.3.4 `string Page::list ( )`

Returns a list of valid books.

##### Returns

files

#### 3.3.3.5 `int Page::next ( string id )`

Returns the next unused page num for a book.

##### Parameters

<i>id</i>	Book ID
-----------	---------

**Returns**

(int)pagenum

**3.3.3.6 string Page::read ( int page, string id )**

Get the ciphertext page from a given book.

**Parameters**

<i>page</i>	Page num
<i>id</i>	Book ID

**Returns**

ciphertext

**3.3.3.7 bool Page::write ( int page, string id, string ciphertext )**

The documentation for this class was generated from the following files:

- [page.h](#)
- [page.cpp](#)

## 3.4 Rand Class Reference

This class provides all secure random routines.

```
#include <rand.h>
```

**Public Member Functions**

- [Rand \(\)](#)  
*The Rand constructor generate a new random seed.*
- unsigned long [getTicks \(\)](#)  
*This function get the tick number from the CPU.*
- void [setSeed \(float\)](#)  
*Random seed setter.*
- float [getSeed \(\)](#)  
*Random sed getter.*
- float [genSeed \(\)](#)
- char [getChar \(\)](#)
- char [getLetter \(\)](#)  
*Get a random [A-Z] char.*
- int [getNumber \(int\)](#)  
*Get a random number.*

### 3.4.1 Detailed Description

This class provides all secure random routines.



### 3.4.2 Constructor & Destructor Documentation

#### 3.4.2.1 Rand::Rand ( )

The [Rand](#) constructor generate a new random seed.

Returns

[Rand](#) object

### 3.4.3 Member Function Documentation

#### 3.4.3.1 float Rand::genSeed ( )

Parameters

<i>Generate</i>	a new seed using some black magic
-----------------	-----------------------------------

Returns

(float)seed

```
seed = (float)( (usecs.tv_usec + getpid()) ^ (int(Rand::getTicks()) << 16) / 10000 );
```

#### 3.4.3.2 char Rand::getChar ( )

Parameters

<i>Get</i>	a random char
------------	---------------

Returns

(char)rnd

#### 3.4.3.3 char Rand::getLetter ( )

Get a random [A-Z] char.

Returns

(char)rnd

#### 3.4.3.4 int Rand::getNumber ( int a )

Get a random number.

Parameters

<i>a</i>	number len
----------	------------

Returns

(int)rnd

### 3.4.3.5 float Rand::getSeed ( )

Random seed getter.

#### Returns

(float)seed

### 3.4.3.6 unsigned long Rand::getTicks ( )

This function get the tick number from the CPU.

#### Returns

(ulong)tsc

In ix86 and amd64 uses RDTSC to get the low ticks value.

In ARMv6 and ARMv7 currently uses a gettimeofday()

### 3.4.3.7 void Rand::setSeed ( float a )

Random seed setter.

#### Parameters

a	The new seed
---	--------------

The documentation for this class was generated from the following files:

- [rand.h](#)
- [rand.cpp](#)

## 3.5 Text Class Reference

[Text](#) and encoding related functions.

```
#include <text.h>
```

### Public Member Functions

- void [replaceAll](#) (string &, const string &, const string &)  
*Replace all characters from a string.*
- void [create](#) (int, string, string, string)  
*Set the [Text](#) object parameters.*
- string [print](#) (int)  
*Print a human friendly [Text](#) object.*
- string [encodeB26](#) (unsigned char \*, long)  
*Returns the text encoded in Base26.*
- void [decodeB26](#) (unsigned char \*, string)  
*Returns the text decoded in Base26.*
- void [parse](#) (string)  
*Parse and set the [Text](#) object with a formatted (headed) message.*

## Public Attributes

- string [msg](#)  
*Message string.*
- string [book](#)  
*Book ID.*
- string [from](#)  
*Sender identificative string (3 letters, for example: AVD)*
- int [page](#)  
*Page num (int)*

### 3.5.1 Detailed Description

[Text](#) and encoding related functions.

### 3.5.2 Member Function Documentation

#### 3.5.2.1 void Text::create ( int *page*, string *book*, string *from*, string *msg* )

Set the [Text](#) object parameters.

##### Parameters

<i>page</i>	<a href="#">Page</a> num
<i>book</i>	Book ID
<i>from</i>	A sender id for identification
<i>msg</i>	The cleartext message

#### 3.5.2.2 void Text::decodeB26 ( unsigned char \* *output*, string *text* )

Returns the text decoded in Base26.

##### Parameters

<i>output</i>	<a href="#">Text</a> decoded
<i>text</i>	Encoded text

#### 3.5.2.3 string Text::encodeB26 ( unsigned char \* *text*, long *len* )

Returns the text encoded in Base26.

##### Parameters

<i>text</i>	<a href="#">Text</a> to encode
<i>len</i>	<a href="#">Text</a> len

##### Returns

Encoded text (string)

#### 3.5.2.4 void Text::parse ( string *text* )

Parse and set the [Text](#) object with a formatted (headed) message.

## Parameters

<i>text</i>	The formatted message string
-------------	------------------------------

3.5.2.5 string Text::print ( int *spa* )

Print a human friendly [Text](#) object.

## Parameters

<i>spa</i>	Space num
------------	-----------

## Returns

sout.str()

## 3.5.2.6 void Text::replaceAll ( string &amp; , const string &amp; , const string &amp; )

Replace all characters from a string.

replaceAll( str, from, to )

## Parameters

<i>str</i>	The string pointer
<i>from</i>	Character to be replaced
<i>to</i>	Replace character

## 3.5.3 Member Data Documentation

## 3.5.3.1 string Text::book

Book ID.

## 3.5.3.2 string Text::from

Sender identificative string (3 letters, for example: AVD)

## 3.5.3.3 string Text::msg

Message string.

## 3.5.3.4 int Text::page

[Page](#) num (int)

The documentation for this class was generated from the following files:

- [text.h](#)
- [text.cpp](#)

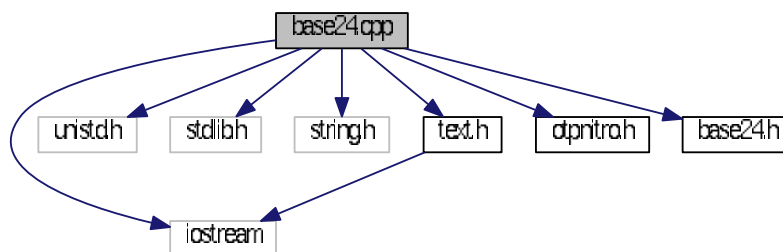
# Chapter 4

## File Documentation

### 4.1 base24.cpp File Reference

```
#include <iostream>
#include <unistd.h>
#include <stdlib.h>
#include <string.h>
#include "text.h"
#include "otpnitro.h"
#include "base24.h"
```

Include dependency graph for base24.cpp:



### Functions

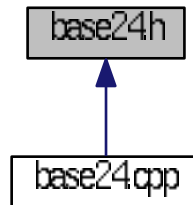
- int [main](#) (int argc, char \*\*argv)

#### 4.1.1 Function Documentation

4.1.1.1 int [main](#) ( int *argc*, char \*\* *argv* )

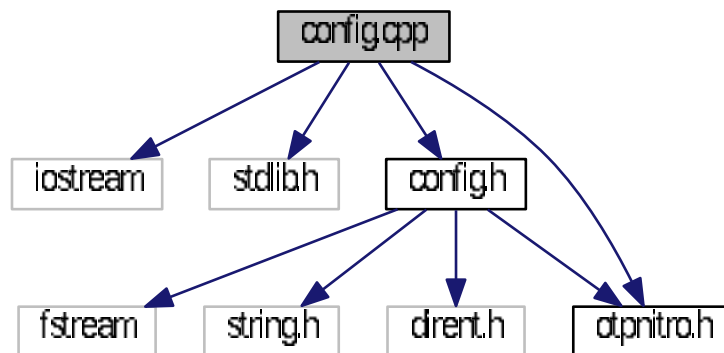
## 4.2 base24.h File Reference

This graph shows which files directly or indirectly include this file:



## 4.3 config.cpp File Reference

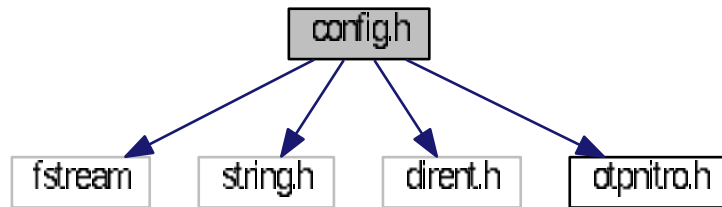
```
#include <iostream>
#include <stdlib.h>
#include "config.h"
#include "otpnitro.h"
Include dependency graph for config.cpp:
```



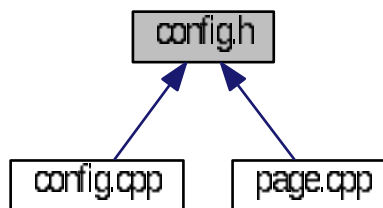
## 4.4 config.h File Reference

```
#include <fstream>
#include <string.h>
#include <dirent.h>
#include "otpnitro.h"
```

Include dependency graph for config.h:



This graph shows which files directly or indirectly include this file:



## Classes

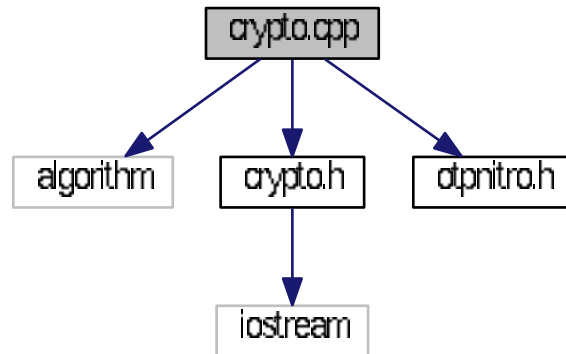
- class [Config](#)

*Configuration, path and pages management.*

## 4.5 crypto.cpp File Reference

```
#include <algorithm>
#include "crypto.h"
#include "otpnitro.h"
```

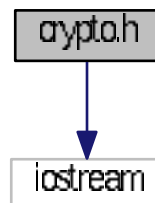
Include dependency graph for crypto.cpp:



## 4.6 crypto.h File Reference

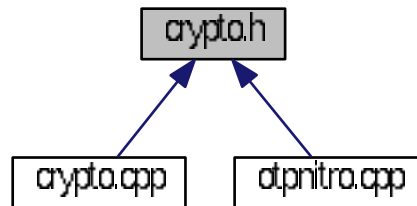
```
#include <iostream>
```

Include dependency graph for crypto.h:





This graph shows which files directly or indirectly include this file:



## Classes

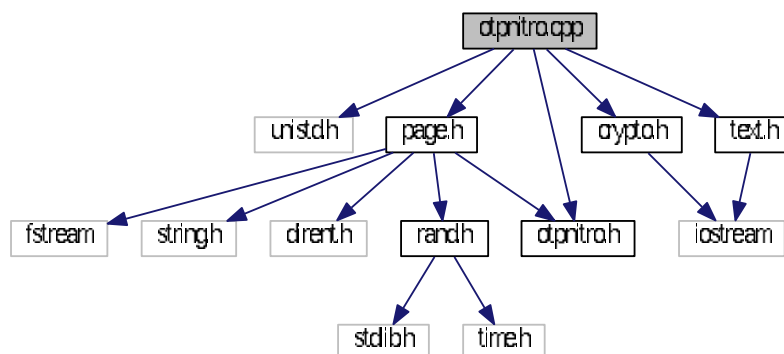
- class [Crypto](#)

*Crypt and decrypt class.*

## 4.7 otpnitro.cpp File Reference

```
#include <unistd.h>
#include "page.h"
#include "crypto.h"
#include "text.h"
#include "otpnitro.h"
```

Include dependency graph for otpnitro.cpp:



## Functions

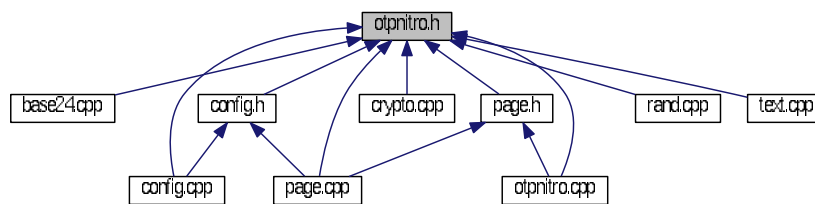
- int [main](#) (int argc, char \*\*argv)

## 4.7.1 Function Documentation

4.7.1.1 `int main ( int argc, char ** argv )`

## 4.8 otpnitro.h File Reference

This graph shows which files directly or indirectly include this file:



## Macros

- `#define VERSION 0.4`
- `#define SPACING 5`
- `#define MAX_PATH 256`

### 4.8.1 Macro Definition Documentation

4.8.1.1 `#define MAX_PATH 256`

4.8.1.2 `#define SPACING 5`

4.8.1.3 `#define VERSION 0.4`

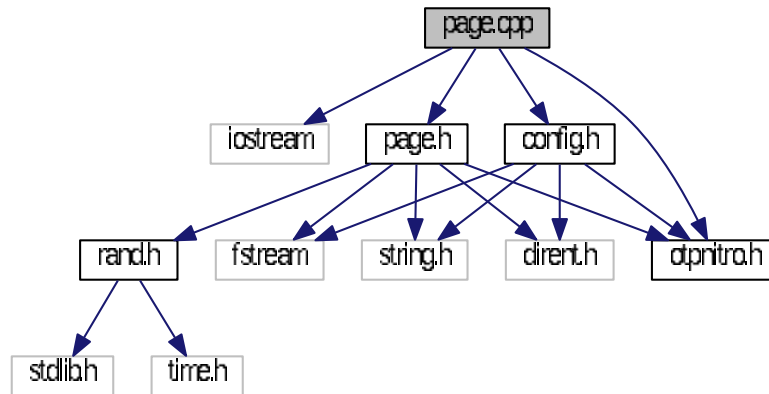
## 4.9 page.cpp File Reference

```

#include <iostream>
#include "page.h"
#include "config.h"
#include "otpnitro.h"

```

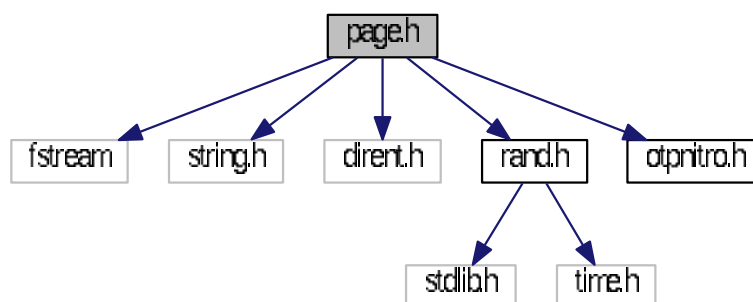
Include dependency graph for page.cpp:



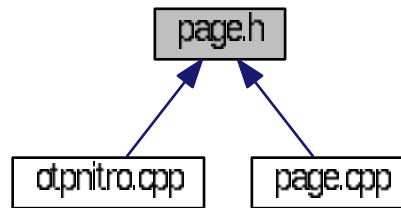
## 4.10 page.h File Reference

```
#include <fstream>
#include <string.h>
#include <dirent.h>
#include "rand.h"
#include "otpnitro.h"
```

Include dependency graph for page.h:



This graph shows which files directly or indirectly include this file:



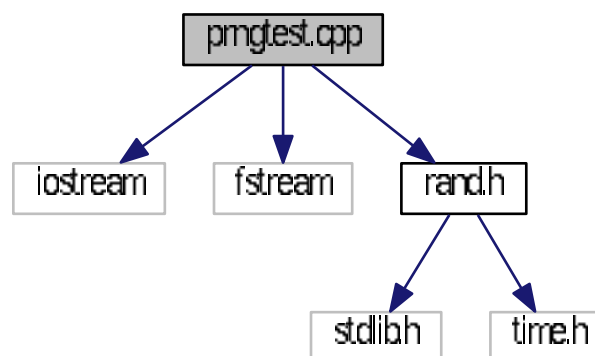
## Classes

- class [Page](#)  
*Page operations class.*

## 4.11 prngtest.cpp File Reference

```
#include <iostream>
#include <fstream>
#include "rand.h"
```

Include dependency graph for prngtest.cpp:



## Macros

- #define [LOOPCNT](#) 1000000

## Functions

- int [main](#) ()

### 4.11.1 Macro Definition Documentation

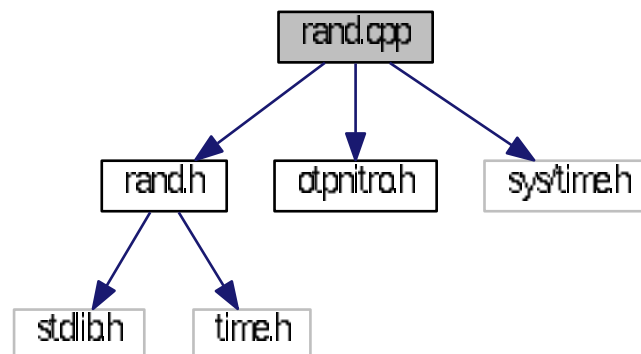
4.11.1.1 `#define LOOPCNT 1000000`

### 4.11.2 Function Documentation

4.11.2.1 `int main ( )`

## 4.12 rand.cpp File Reference

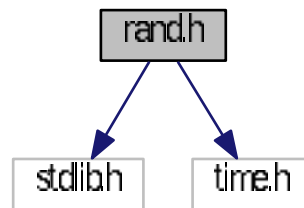
```
#include "rand.h"  
#include "otpnitro.h"  
#include <sys/time.h>  
Include dependency graph for rand.cpp:
```



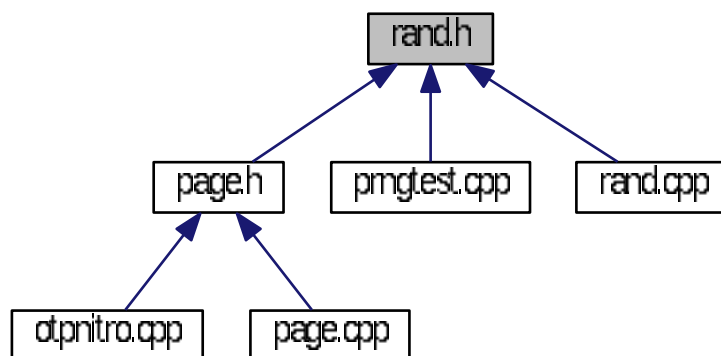
## 4.13 rand.h File Reference

```
#include <stdlib.h>  
#include <time.h>
```

Include dependency graph for rand.h:



This graph shows which files directly or indirectly include this file:



## Classes

- class [Rand](#)

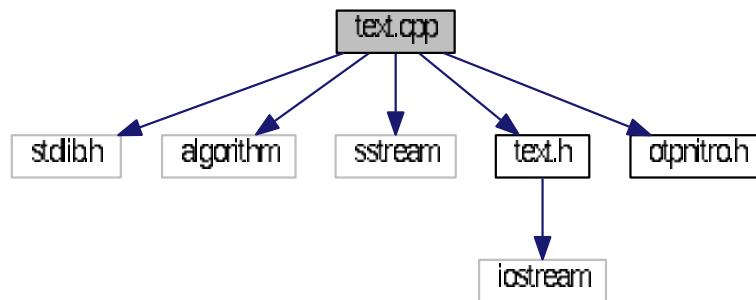
*This class provides all secure random routines.*

## 4.14 text.cpp File Reference

```

#include <stdlib.h>
#include <algorithm>
#include <sstream>
#include "text.h"
#include "otpnitro.h"
  
```

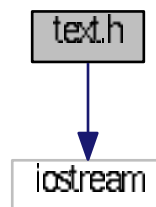
Include dependency graph for text.cpp:



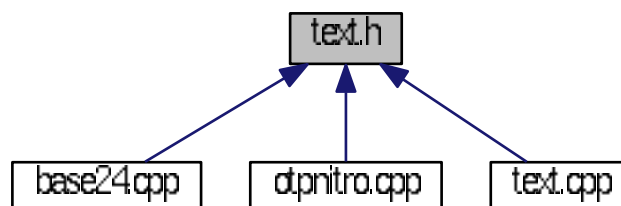
## 4.15 text.h File Reference

```
#include <iostream>
```

Include dependency graph for text.h:



This graph shows which files directly or indirectly include this file:



## Classes

- class [Text](#)  
*Text and encoding related functions.*



# Index

- base24.cpp, 15
  - main, 15
- base24.h, 16
- book
  - Text, 14
- burn
  - Page, 9
- Config, 5
  - Config, 5
  - getChars, 6
  - getPages, 6
  - getPath, 6
  - saveConfig, 6
  - setChars, 6
  - setPages, 6
  - setPath, 7
- config.cpp, 16
- config.h, 16
- create
  - Text, 13
- Crypto, 7
  - decrypt, 7
  - encrypt, 7
- crypto.cpp, 17
- crypto.h, 18
- decodeB26
  - Text, 13
- decrypt
  - Crypto, 7
- encodeB26
  - Text, 13
- encrypt
  - Crypto, 7
- from
  - Text, 14
- genSeed
  - Rand, 11
- generate
  - Page, 9
- get
  - Page, 9
- getChar
  - Rand, 11
- getChars
  - Config, 6
- getLetter
  - Rand, 11
- getNumber
  - Rand, 11
- getPages
  - Config, 6
- getPath
  - Config, 6
- getSeed
  - Rand, 11
- getTicks
  - Rand, 12
- LOOPCNT
  - prngtest.cpp, 23
- list
  - Page, 9
- MAX\_PATH
  - otpnitro.h, 20
- main
  - base24.cpp, 15
  - otpnitro.cpp, 20
  - prngtest.cpp, 23
- msg
  - Text, 14
- next
  - Page, 9
- otpnitro.cpp, 19
  - main, 20
- otpnitro.h, 20
  - MAX\_PATH, 20
  - SPACING, 20
  - VERSION, 20
- Page, 8
  - burn, 9
  - generate, 9
  - get, 9
  - list, 9
  - next, 9
  - Page, 8
  - read, 10
  - write, 10
- page
  - Text, 14
- page.cpp, 20
- page.h, 21
- parse
  - Text, 13

print  
  Text, [14](#)

prngtest.cpp, [22](#)  
  LOOPCNT, [23](#)  
  main, [23](#)

Rand, [10](#)  
  genSeed, [11](#)  
  getChar, [11](#)  
  getLetter, [11](#)  
  getNumber, [11](#)  
  getSeed, [11](#)  
  getTicks, [12](#)  
  Rand, [11](#)  
  setSeed, [12](#)

rand.cpp, [23](#)  
rand.h, [23](#)

read  
  Page, [10](#)

replaceAll  
  Text, [14](#)

SPACING  
  otpnitro.h, [20](#)

saveConfig  
  Config, [6](#)

setChars  
  Config, [6](#)

setPages  
  Config, [6](#)

setPath  
  Config, [7](#)

setSeed  
  Rand, [12](#)

Text, [12](#)  
  book, [14](#)  
  create, [13](#)  
  decodeB26, [13](#)  
  encodeB26, [13](#)  
  from, [14](#)  
  msg, [14](#)  
  page, [14](#)  
  parse, [13](#)  
  print, [14](#)  
  replaceAll, [14](#)

text.cpp, [24](#)  
text.h, [25](#)

VERSION  
  otpnitro.h, [20](#)

write  
  Page, [10](#)