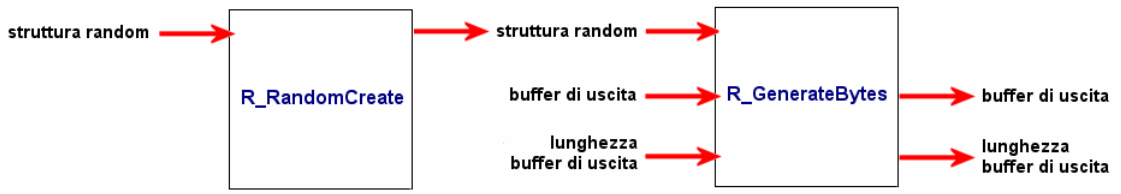
Network Security
Elements of Applied Cryptography

The RSAEuro library

RSAEURO TOOLKIT

- RSAEuro is cryptographic toolkit developed in the C/C++ language and provided by Reaper Technologies (http://www.reapertech.com)
- The Internet release provides the following functionalities:
  - RSA encryption, decryption and key generation (compatible con PKCS#1)
  - MD2, MD4, MD5
  - DES in modalità CBC (1, 2 or 3 keys using Encrypt-Decrypt-Encrypt)
  - Diffie-Hellman key agreement as defined in PKCS #3.
  - PEM support support for RFC 1421 encoded ASCII data with all main functions.
  - Key routines implemented in assembler for speed (80386 and 680x0 currently supported).

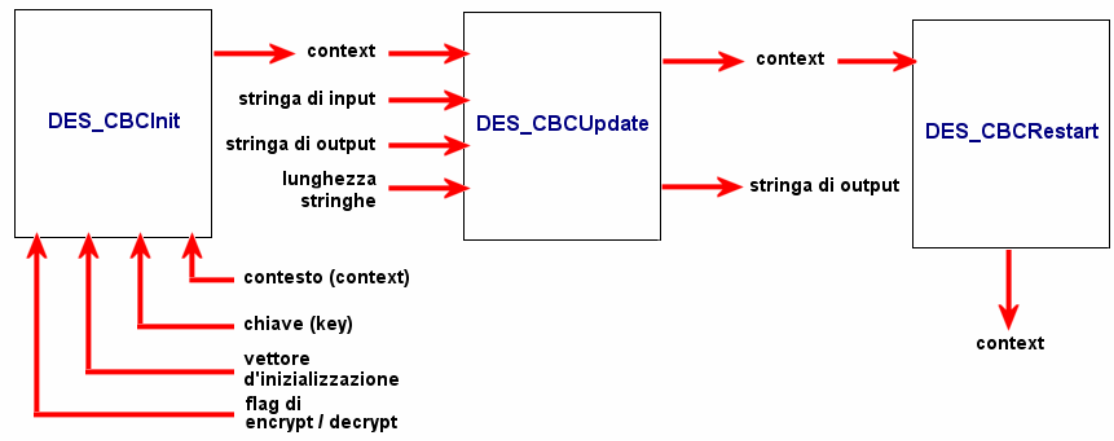
Random numbers




```
void R_RandomCreate(random)
R_RANDOM_STRUCT *random;

int R_GenerateBytes(block, len, random)
unsigned char *block;
unsigned int len;
R_RANDOM_STRUCT *random;
```

DES in the CBC mode

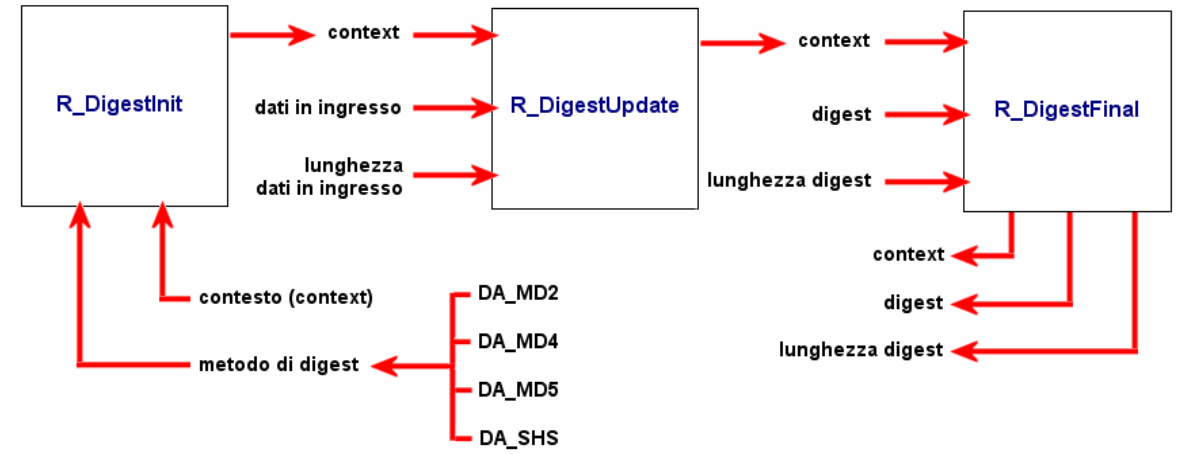


DES in the CBC mode

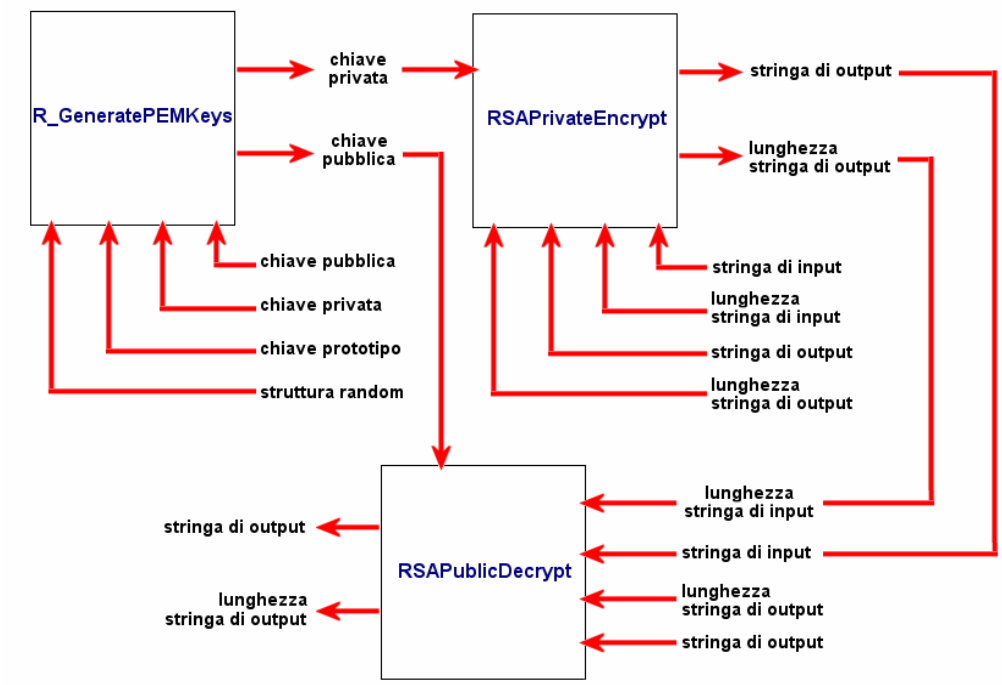
```
void DES_CBCInit(context, key, iv, encrypt)
DES_CBC_CTX *context;
unsigned char *key;
unsigned char *iv;
int encrypt;
```

```
int DES_CBCUpdate(context, output, input, len)
DES_CBC_CTX *context;
unsigned char *output;
unsigned char *input;
unsigned int len;
```

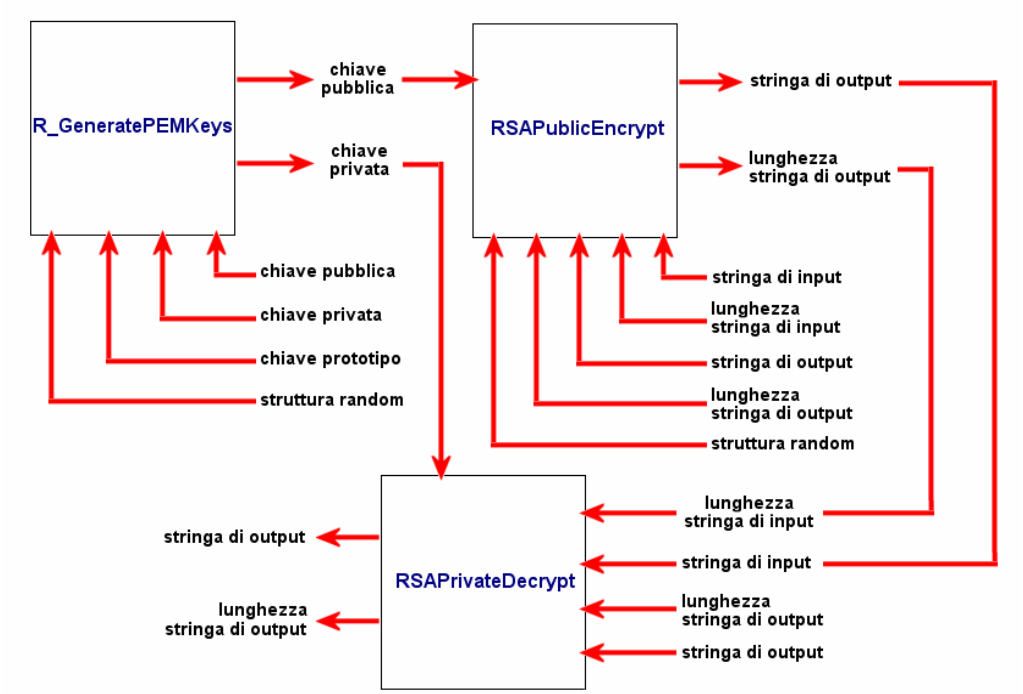
Digest



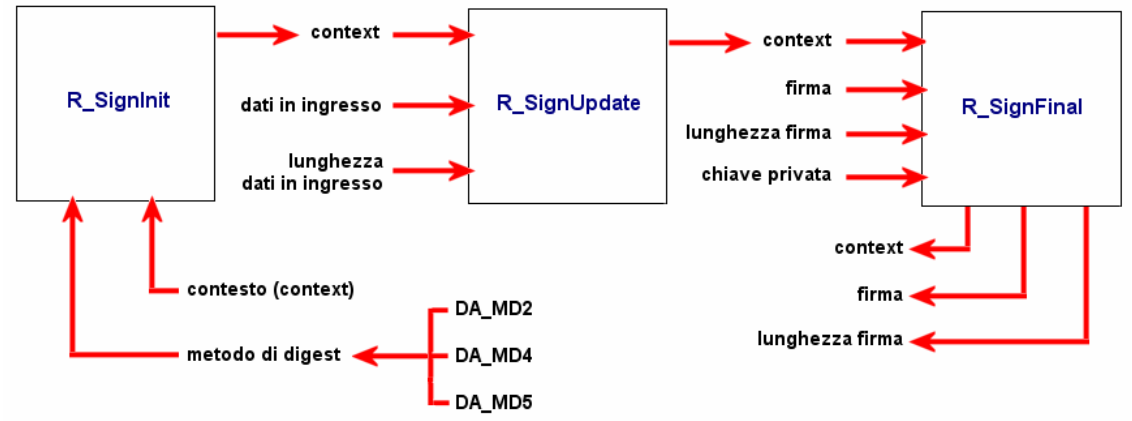
RSA (encryption)



RSA (encryption)



Digital signature: signature generation



Digital signature: signature verification