# Cryptology

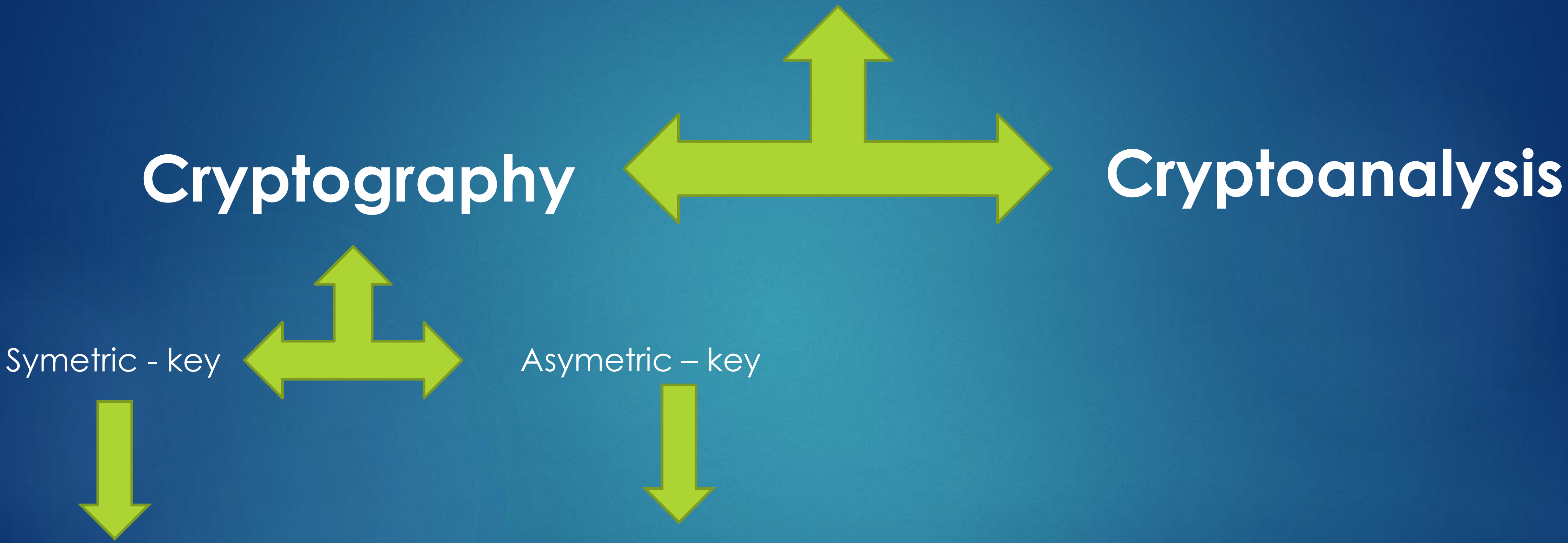
JAKUB BOJKO 2V

"Kryptos" (greek) - Hidden/Secret

"Logia" (greek) - study

# Cryptology

# CRYPTOLOGY



Cryptography

Cryptoanalysis

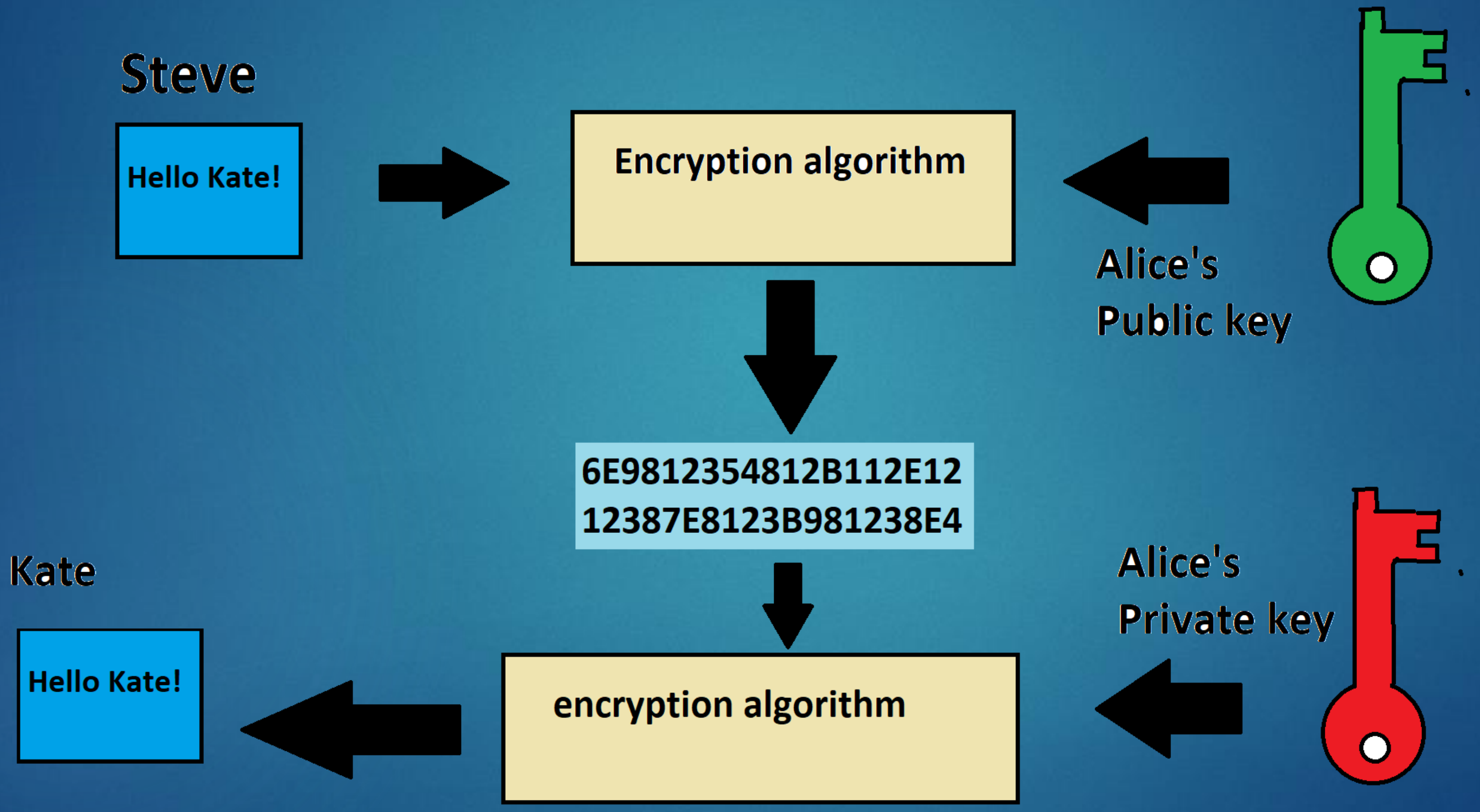
Symetric - key

Asymetric – key

- AES (Advanced Encryption Standard)
- DES ( Data Encryption Standard)
- RC4 (Rivest Cipher 4)
- IDEA (International Data Encryption Algorithm)

- RSA (Rivest-Shamir- adleman)
- DSA (Digital Signature Algorithm)

# RSA Cryptosystem (asymetric key)



Steve

Hello Kate!

Encryption algorithm

Alice's Public key

6E9812354812B112E12
12387E8123B981238E4

Kate

Hello Kate!

encryption algorithm

Alice's Private key

# Role of Math in cryptology (RSA)

- 1. Chose 2 different odd values for variables "**P**" and "**Q**"
- 2. Calculate variable "**N**", by using this formula: **N = (P*Q)**
- 3. Calculate variable "**f**" by using this formula: **f=(p-1)*(q-1)**
- 4. Find the lowest possible number, that is relatively prime towards variable "**f**" (e=7 is the lowest prime number relatively towards 120). Then assign that number to a variable "**d**"
- 5. Find variable "**d**" by using this equation: **e*d(mod f) = 1(mod f)**

  "A(mod B)" - remainder from dividing **A** by **B**
- 6. Form your Private key as follows: **Private key - (e, n)**
- 7. Form your public key as follows: **Public key - (d, n)**

## In order to encrypt a message:

C - number you want to encrypt
M – encrypted number

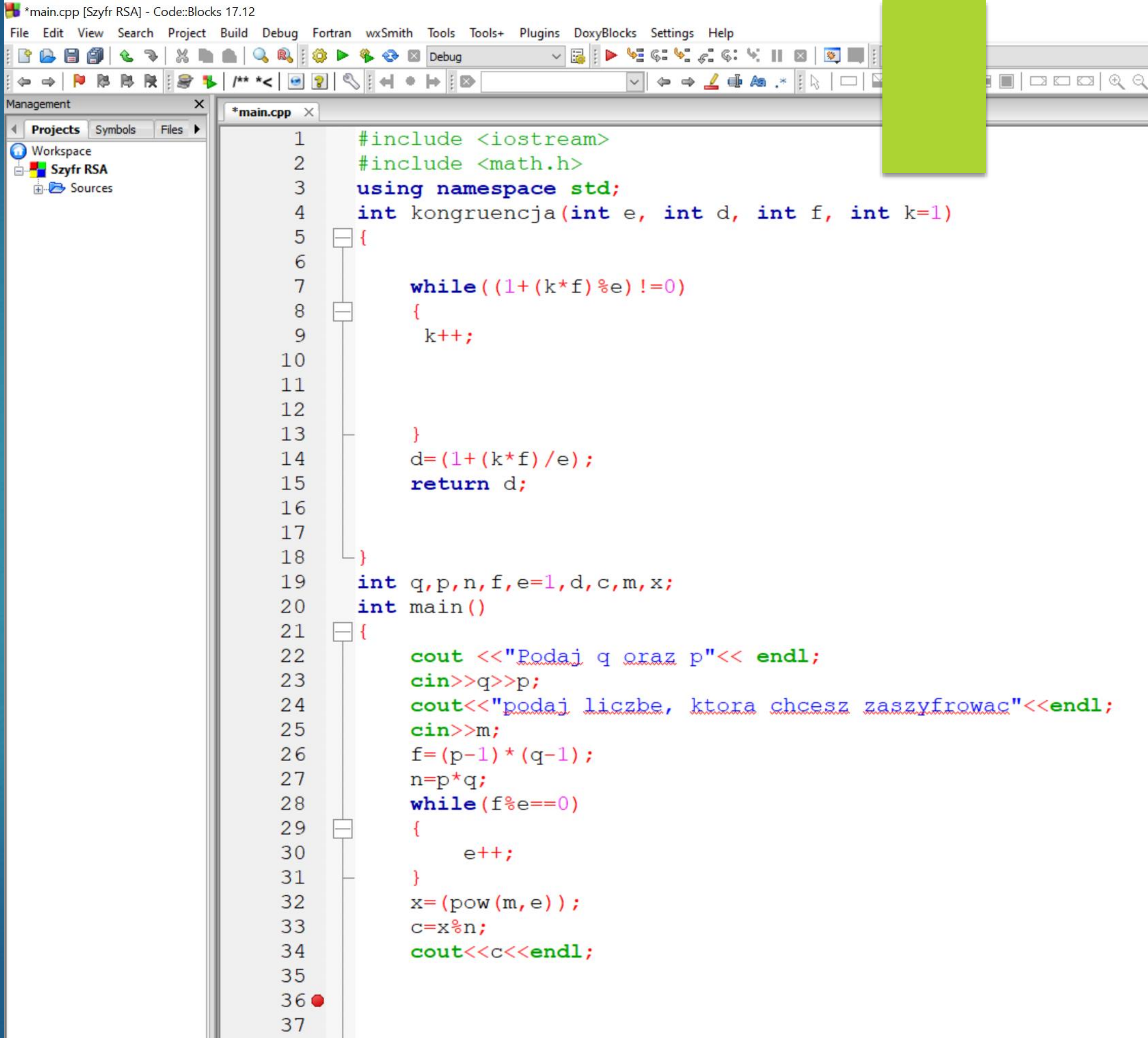
**Formula:** $c = m^e (mod\ n).$

## In order to decrypt a message:

C - number you want to encrypt
M – encrypted number

**Formula:** $m = c^d (mod\ n)$

# RSA Encryption programmed


*main.cpp [Szyfr RSA] - Code::Blocks 17.12
File Edit View Search Project Build Debug Fortran wxSmith Tools Tools+ Plugins DoxyBlocks Settings Help
Debug
Management
Projects Symbols Files
Workspace
Szyfr RSA
Sources
*main.cpp

```cpp
#include <iostream>
#include <math.h>
using namespace std;
int kongruencja(int e, int d, int f, int k=1)
{

    while((1+(k*f)%e)!=0)
    {
     k++;



    }
    d=(1+(k*f)/e);
    return d;


}
int q,p,n,f,e=1,d,c,m,x;
int main()
{
    cout <<"Podaj q oraz p"<< endl;
    cin>>q>>p;
    cout<<"podaj liczbe, ktora chcesz zaszyfrowac"<<endl;
    cin>>m;
    f=(p-1)*(q-1);
    n=p*q;
    while(f%e==0)
    {
        e++;
    }
    x=(pow(m,e));
    c=x%n;
    cout<<c<<endl;


```

# Applications of cryptology in modern world

Mails

Bankery

Social medias

Military

Passwords and Authentications

Space exploration