UNIVERSITY OF GLOUCESTERSHIRE

CT5046

Mathematics for Cryptography

Week 3 – online session

Dr Adam Gorine

Learning Outcomes – This Session

- Greatest Common Divisor
- Cryptography: The Euclidean Algorithm
- Chinese Remainder Theorem
- Entropy

Greatest Common Divisor

- The greatest common divisor (**GCD**)of two numbers is *the largest number* that divides them both.
- For example the GCD of 20 and 15 is 5, since
  - ✓ 5 divides both 20 and 15 and no larger number has this property.
- The GCD is used for a variety of applications including:
  - ✓ Number theory (https://brilliant.org/wiki/number-theory)
  - ✓ Modular arithmetic and encryption algorithms such RSA

Greatest Common Factor of 12 and 16?

1. Find all the factors of each number
2. Find the ones that are common to both.
3. Choose the Greatest.

Work out the GCF of these numbers

- 6 and 18
- 9 and 12
- 24 and 108

UNIVERSITY OF GLOUCESTERSHIRE

Solution

Numbers	Factors	Common factors	GCF
9	1, 3, 9	1, 3	3
12	1, 2, 3, 4, 6, 12		

Numbers	Factors	Common factors	GCF
6		1, 2, 3, 6	6
18	1, 2, 3, 6, 9, 18		

We can use the prime factors

Numbers	Factors	CGF
24	2 x 2 x 2 x 3	**2 x 2 x 3 = 12**
108	2 x 2 x 3 x 3 x 3	

Euclidean Algorithm

It is an algorithm for finding the greatest common divisor of two positive numbers, **a** and **b**.

For example, let assume **a=210** and **b=45**

- Divide **210** by **45**, and get the result 4 with remainder 30, so 210=4 x 45 + 30.
- Divide **45** by **30**, and get the result 1 with remainder 15, so 45=1 **x** 30 + 15.
- Divide **30** by **15**, and get the result 2 with remainder 0, so 30 = 2 **x** 15 + 0.
- The greatest common divisor of **210** and **45** is **15.**

Formal description of the Euclidean algorithm

The Euclidean Algorithm for finding GCD(A,B) is as follows:

- If A = 0 then GCD(A,B)=B, since the GCD(0,B)=B, and we can stop.
- If B = 0 then GCD(A,B)=A, since the GCD(A,0)=A, and we can stop.
- Write A in quotient remainder form ($A = B \cdot Q + R$)
- Find GCD(B,**R**) using the Euclidean Algorithm since GCD(A,B) = GCD(B,**R**)

Work out the GCD(270,192)

Using Euclidean Algorithm

Work out the GCD(270,192) using Euclidean Algorithm

Step 1: **A=270**, B=192

- A ≠0
- B ≠0
- Use long division to find that 270/192 = 1 with a remainder of 78.
  We can write this as: 270 = **192** * 1 +**78**
- Find GCD(192,78), since GCD(270,192)=GCD(**192**,**78**)

Work out the GCD(270,192) using Euclidean Algorithm

Step 2: **A=192**, B=78

- A ≠0
- B ≠0
- Use long division to find that 192/78 = 2 with a remainder of **36**.
  We can write this as: 192= **78** * 2 + **36**
- Find GCD(78,36), since GCD(192, 78)=GCD(78, **36**)

Work out the GCD(270,192) using Euclidean Algorithm

Step 3: **A=78**, B=36

- A ≠0
- B ≠0
- Use long division to find that 78/36 = 2 with a remainder of **6**.
  We can write this as: 78 = **36** * 2 + **6**
- Find GCD(36, 6), since GCD(78, 36)=GCD(36, **6**)

Work out the GCD(270,192) using Euclidean Algorithm

Step 4: **A=36**, B=6

- $A \neq 0$
- $B \neq 0$
- Use long division to find that 36/6 = 6 with a remainder of **0**.
  We can write this as: 36 = **6** * 6 + **0**
- Find GCD(6, 0), since GCD(36, 6)=GCD(6, **0**)

Work out the GCD(270,192) using Euclidean Algorithm

Step 5: **A=6**, B=0

- A $\neq$0
- B = 0, GCD(6, 0) = 6

- We have shown:

GCD(270,192) = GCD(192,78) = GCD(78,36) = GCD(36,6) = GCD(6,0) = 6

GCD (270, 192) = 6

What is modular arithmetic

Congruence: $a \equiv b \pmod{n}$

Given two numbers **a** and **b**, we say that a and b are congruent with respect to **n** if:

1) **a** and **b** have the same remainder when they are divided by **n**.
2) **a** = **k**.**n** + **b**
3) **n** |(**a**-**b**) "**n** divides (a-b)" i.e (a-b) is multiple of n.

Examples of congruence

- 2 and 12 are congruent with respect to 10 since

$$2 \equiv 12 \ (mod\ 10)$$

- Similarly 3 and 6 are congruent with respect to 3 since

$$3 \equiv 6 \ (mod\ 3)$$

Chinese reminder theorem

- If we have a set of congruences such that:

$$x \equiv a_1 \; (mod \;\; m_1)$$
$$x \equiv a_2 \; (mod \;\; m_2)$$
$$\vdots$$
$$x \equiv a_k \; (mod \;\; m_k)$$

- There is exactly one solution $x \in Z_m$ satisfying all of them.

Conditions

1. $gcd(m_i, m_j) = 1$
2. $m = m_i \times m_2 \times m_3 .., \times m_k$
3. $a_1, a_2, ..., a_k$ and $m_1, m_2, ..., m_k$ are integers

How it works

- Step 1: For each z_i in $z_1, z_2, ..., z_k$, calculate $z_i = m/m_i$
- Step 2: For each y_i in $z_1, z_2, ..., z_k$, calculate $y_i = z_i^{-1} (mod \ m_i)$
- Step 3: The value of x then becomes $x = a_1 y_1 z_1 + .. + a_k y_k z_k$

Example

Imagine that we want to find the value of x in Z_{60} such that

$$\begin{aligned} x &\equiv 3 \ (mod \ 4) \\ x &\equiv 2 \ (mod \ 3) \\ x &\equiv 4 \ (mod \ 5) \end{aligned}$$

Step 0 - Initialise: $a_1 = 3$, $a_2 = 2$, $a_3 = 4$, $m_1 = 4$, $m_2 = 3$, $m_3 = 5$, $m = 4 \times 3 \times 5 = 60$

Example (cont...)

Step 1: Calculate $z_1 = m/m_1 = 60/4 = 15$, $z_2 = 20$, and $z_3 = 12$
Step 2: Calculate the module inverse $z_i y_i \equiv 1 \ mod \ m_i$. In other words, we want to solve the following:

$$15y_1 \equiv 1 \ mod \ 4$$
$$20y_2 \equiv 1 \ mod \ 3$$
$$12y_3 \equiv 1 \ mod \ 5$$

Based on calculations, $y_1 = 3, y_2 = 2$, and $y_3 = 3$

Example (cont...)

Step 3: Finally calculate the value x by:

$$x \equiv a_1 y_1 z_1 + \ a_2 y_2 z_2 \ + \ a_3 y_3 z_3 \ (\ mod \ 60)$$

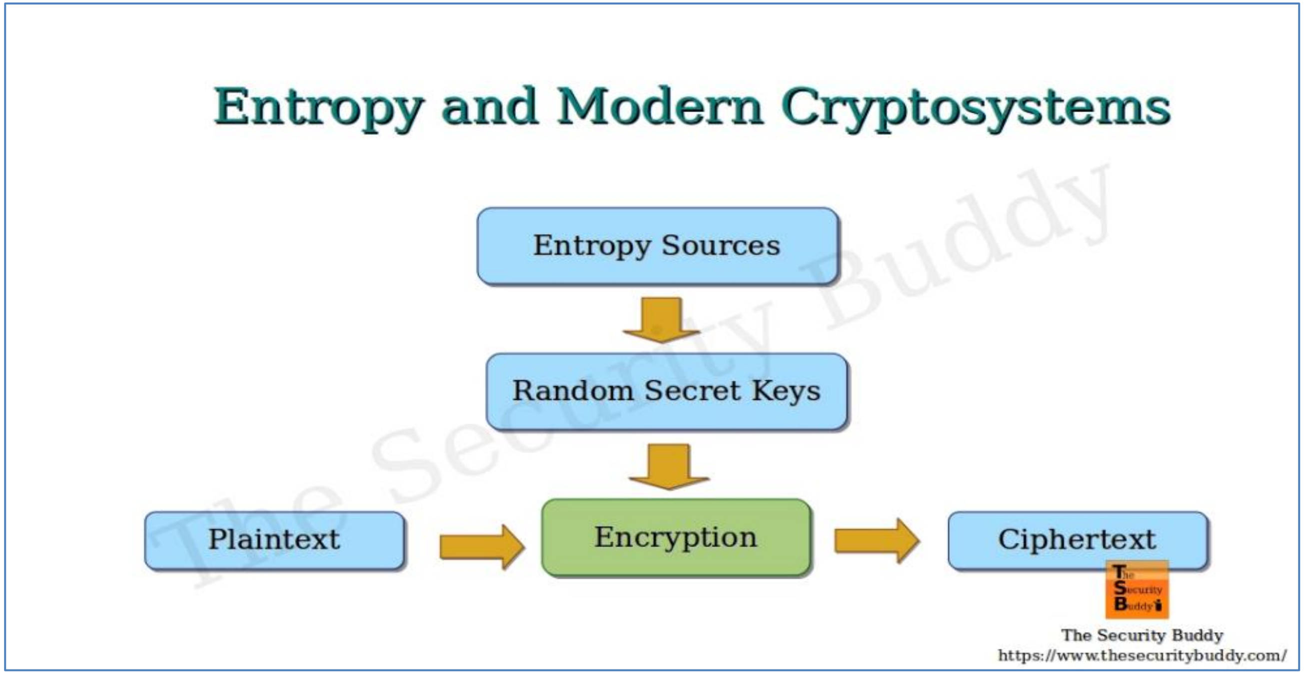
$$x \equiv 3 \times 3 \times 15 + 2 \times 2 \times 20 \ + \ 4 \times 3 \times 12 \ (\ mod \ 60)$$

$$x \equiv 59 \ (mod \ 60)$$

ENTROPY

- In information theory, ***entropy*** is a measure of *unpredictability* of information contained in a message.

What is entropy in cryptography?



Entropic security is used to indicate how difficult it is for an attacker to extract meaningful information about the plaintext from the ciphertext when he does not know the secret key.

Homework

Using the Chinese reminder theorem, calculate x

X = 2 (mod 3)

X = 2 (mod 4)

X = 1 (mod 5)

Find X.

Any Questions?