**Practical Session 5**

*Kid Krypto*

"Kid Krypto" [1] is a family of cryptosystems developed by Michael Fellows and Neal Koblitz for the teaching of cryptography without using advanced mathematics.

Kid Krypto uses two different but related keys for encryption and decryption. To set up Kid Krypto, Alice chooses four random integers *a*, *b*, *A* and *B*. She then computes:

She makes the pair *(n, e)* available as her public key and keeps *d* as her private key. All the other numbers can be discarded; at any moment they should never be revealed. Messages in this system are integers *x  n*.

Suppose Bob wishes to send message *x* to Alice. He encrypts it by first multiplying *x* by *e*, and dividing the product *xe* by *n*. The remainder of this division is the ciphertext *y*. Alice decrypts *y* by multiplying by *d* to obtain *yd*, then dividing this product by *n*. The remainder of this division is the plaintext.

To see this in action, suppose that Alice choose

Then it is easy to determine

Her public key is *(369,58)*, and her private key is *70*.

Suppose Bob wants to encrypt*x=200*. He multiplies by *e=58* to obtain *xe= 11600*. Dividing by *n=369* leaves a remainder of *161*. This is the ciphertext *y* he sends to Alice.

Alice multiplies this ciphertext *y=161* by *d=70* to obtain *yd=11270*. She then divides by *n* to obtain a remainder of *200*, which is the required plaintext.

For this system to be secure, there should be no way that Bob (or anyone else) can easily determine the value of d from the public values *n* and *e*. He knows that , but he does not know *M*.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Testing Vectors** | | | | | |
| **a** | **b** | **A** | **B** | **Plaintext** | **Ciphertext** |
| 3 | 4 | 5 | 6 | 200 | 161 |
| 3 | 4 | 5 | 6 | 650 | 62 |
| 9 | 11 | 5 | 8 | 1028 | 572 |
| 9 | 11 | 5 | 8 | 54 | 2546 |
| 47 | 22 | 11 | 5 | 12223 | 13268 |
| 47 | 22 | 11 | 5 | 4356 | 28929 |

**Activity**

1. Use Kid Krypto with values *a = 10, b = 2, A = 15, B = 5* to encrypt *x = 112.*
2. Answer the following questions.
   1. All integers can be chosen to set up Kid Krypto? Why
   2. If you answer no in the previous question, say which numbers cannot be used and why
3. Upload a file with all that findings individually.

**Implementation**

1. Make your individual submission on Alphagrader your implementation in the programming language of your choice.

**References**

[1]. Michael Fellows and Neal Koblitz. Kid Krypto. In Ernest Brickwell, editor, *Advances in Cryptology CRYPTO 92,* Volume 740 of *Lecture Notes in Computer Science*, pages 371-389. Springer, 1993