Department of Computer Science — University of Wisconsin-Whitewater
Cryptography and Cloud Security Midterm Exam

Dr. Jiazhen Zhou

Abdoul-Nourou Yigo

March 2019

1 Congruential Algorithm

$X_{n+1} = 7X_n \mod 13$

1. Assume that $X_0 = 1$, write out the sequence till a number is repeated in the sequence. Does this generate a full period?

   $X_0 = 1$
   $X_1 = 7 \times \mod 13 = 7$
   $X_2 = 7 \times 7 \mod 13 = 10$
   $X_3 = 7 \times 10 \mod 13 = 5$
   $X_4 = 7 \times 5 \mod 13 = 9$
   $X_5 = 7 \times 9 \mod 13 = 11$
   $X_6 = 7 \times 11 \mod 13 = 12$
   $X_7 = 7 \times 12 \mod 13 = 6$
   $X_8 = 7 \times 6 \mod 13 = 3$
   $X_9 = 7 \times 3 \mod 13 = 8$
   $X_{10} = 7 \times 8 \mod 13 = 4$
   $X_{11} = 7 \times 4 \mod 13 = 2$
   $X_{12} = 7 \times 2 \mod 13 = 1$

   With the above result we can see the sequence repeats at X_{12}; therefore, it generates a full period.

2. Does this sequence look random to you? Hint: if you can find some relationship among neighboring (could be evenly spaced numbers) numbers in the sequence, likely it means that it is not random.

   Let's an observation to analyse the number patterns:

$X_1 - X_0 = 6$

$X_2 - X_1 = 3$

$X_3 - X_2 = 5$

$X_4 - X_3 = 4$

$X_5 - X_4 = 2$

$X_6 - X_5 = 1$

$X_7 - X_6 = 6$

$X_7 - X_8 = 3$

$X_9 - X_8 = 5$

$X_9 - X_{10} = 4$

$X_{11} - X_{10} = 2$

$X_{11} - X_{12} = 1$

When we do a substrations between the values (predecessor and successor) or vice versa we can see that the subtraction results repeat twice in the sequence. Each value repeat at index $i+6$ position for instance. From this observation, we can clearly see a pattern between the numbers generation. We can conclude that this process is not random.

3. Using the keystream generated above (each key is 4 bits) for a stream cipher to encrypt the the plaintext ”ab e4 25 69 3c 2f 8d 21”, what is the ciphertext?

   Plaintext: ab e4 25 69 3c 2f 8d 21
   Keystream: 1 7 10 5 9 11 12 6 3 8 4 2

   Let's effectuate the encryption:

   1010 1011 1110 0100 0010 0101 0110 1001 0011 1100 0010 1111 1000 1101 0010 0001

   0001 0111 1010 0101 1001 1011 1100 0110 0011 1000 0100 0010 0001 0111 1010 0101

   1011 1100 0100 0001 1011 1110 1010 1111 0000 0100 0110 1101 1001 1010 1000 0100

   b c 4 1 b e a f 0 4 6 d 9 a 8 4

   CipherText: bc 41 be af 04 6d 9a 84

4. If the recieved stream cipher is ”45 6c 26 3e 47 5c”, please decrypt the stream. Note that the receiver is using the same pseudo number generator as the sender and knows the same seed (1 in this case).

   $X_1 = 7$

   $X_2 = 7 \times 7 \mod 13 = 10$

   $X_3 = 7 \times 10 \mod 13 = 5$

   $X_4 = 7 \times 5 \mod 13 = 9$

   $X_5 = 7 \times 9 \mod 13 = 11$

   $X_6 = 7 \times 11 \mod 13 = 12$

   $X_7 = 7 \times 12 \mod 13 = 6$

   $X_8 = 7 \times 6 \mod 13 = 3$

   $X_9 = 7 \times 3 \mod 13 = 8$

   $X_{10} = 7 \times 8 \mod 13 = 4$

   $X_{11} = 7 \times 4 \mod 13 = 2$

$X_{12} = 7 \times 2 \mod 13 = 1$
$X_{13} = 7 \times 1 \mod 13 = 7$

CipherText: 45 6c 26 3e 47 5c

Keystream: 7 10 5 9 11 12 6 3 8 4 2 1

0100 0101 0110 1100 0010 0110 0011 1110 0100 0111 0101 1100

0111 1010 0101 1001 1011 1100 0110 0011 1000 0100 0010 0001

0011 1111 0011 0101 1001 1010 0101 1101 1100 0011 0111 1101

3 f 3 5 9 a 5 d c 3 7 d

Plaintext: 3f 35 9a 5d c3 7d

2 Modular Arithmetic Operations

Find the results of the following modular arithmetic operations. Use related theorem (e.g Euler's theoreme) as appropriate.

1. $10^{482} \mod 33$

   $a = 10$
   $n = 33$

   $\phi(33) = (3-1) \times (11-1) = 20$
   $10^{20} \mod 33 = 1$
   $10^{20 \times 24 + 2} \mod 33 = (10^{20})^{24} \times 10^{2} \mod 33 = 1$

2. $8^{602} \mod 39$

   $a = 8$
   $n = 39$
   $\phi(39) = (3-1) \times (13-1) = 24$
   $8^{24} \mod 39 = 1$
   $8^{24 \times 25 + 2} \mod 39 = (8^{24})^{25} \times 8^{2} \mod 39$
   $8^{2} \mod 39 = 25$

3. $6^{163} \mod 17$

   We have $a = 6$, $p = 17$ such that $6^{16} \mod 17 = 1$

   Dividing the exponent by $p - 1$ we have:

   $163 = 16 \times 10 + 3$
   $6^{163} \mod 17 = 6^{16 \times 10 + 3} \mod 17$
   $= 6^{16 \times 10} \times \mod 17 \times 6^{3} \mod 17$
   $= 1^{10} \times 6^{3} \mod 17 = 12$

4. $33^{162} \mod 11$

   We have $a = 33$, $p = 11$ such that $33^{10} \mod 11 = 1$

   Diving the exponent by $p - 1$ we have:

$162 = 10 \times 16 + 2$
$33^{162} \mod 11 = 33^{10 \times 16 + 2} \mod 11$
$= 1 \times 33^2 \mod 11 = 0$

3 RSA Algorithm

For RSA algorithm, find the private key for each of the following case and show your encryption and decryption results with given M

1. $p = 7$, $q = 13$, $e = 29$, $M = 81$

   - Calculation of n
     $n = pq = 7 \times 13 = 91$

   - Calculation of $\phi(n)$
     $\phi(n) = (p-1)(q-1) = (7-1)(13-1) = 72$

   - Calculation of the private key d
     $ed = \phi(n) \times k + 1$
     $29d = 72 \times k + 1$
     $k = 2$
     $d = \frac{145}{29}$
     $d = 5$

   - Encryption procedures
     $C = M^e \mod n$
     $C = 81^{29} \mod 91$
     $C = (81^3)^8 \mod 91 \times 81^4 \mod 91 \times 81 \mod 91$
     $(81^3)^8 \mod 91 = 1$
     $(81^4 \times 81) \mod 91 = 9$
     $C = 9$

   - Procedures for descryption
     $M = C^d \mod 91$
     $M = 9^5 \mod 91$
     $M = 59049 \mod 91$
     $M = 81$

2. $p = 5$, $q = 17$, $e = 3$, $M = 31$

   - Calculation of n
     $n = pq = 5 \times 17 = 85$

   - Calculation of $\phi(n)$
     $\phi(n) = (p-1)(q-1) = (5-1)(17-1) = 64$

- Calculation of the private key d
  $ed = \phi(n) \times k + 1$
  $3d = 64 \times k + 1$
  $k = 2$
  $d = \frac{129}{3}$
  $d = 43$
- Encryption procedures
  $C = M^e \mod n$
  $C = 31^3 \mod 85$
  $C = 29791 \mod 85$
  $C = 41$
- Decrytion procedures
  $M = 41^{43} \mod 85$
  $M = (41^6)^7 \mod \times 41 \mod 85$
  $M = (26^7 \times 41) \mod 85$
  $M = 31$

3. $p = 3$, $q = 19$, $M = 65$

   - Calculation of n
     $n = pq = 3 \times 19 = 57$
   - Calculation of $\phi(n)$
     $\phi(n) = (p-1)(q-1) = (3-1)(19-1) = 36$
   - We could observe that there is a basic requirement that is not met because $M > n$. Therefore, we could conclude that the Encryption and decryption procedures could not be done.

4 Block Cipher Operations

Suppose that one has designed a block cipher operation mode as

$$C_i = E_k(P_{i-1}) \oplus P_i$$
$$P_0 = IV$$

1. Write the formula for decrypting in the receiver side
   $P_i = C_i \oplus D_k(P_{i-1})$
2. Is it possible to execute encryption in parallel? How about decryption? Justify your answer.

   Observing the blocks chaining from $Figure 1$, we could see that the encryption can be done in parallel. It can be done as such because we do not relate on the result of the prodecessor to encrypt the successor ciphertext.

   On the other hand, the decryption cannot be done in parallel because each procedecessor block output is needed to decrypt the next one.

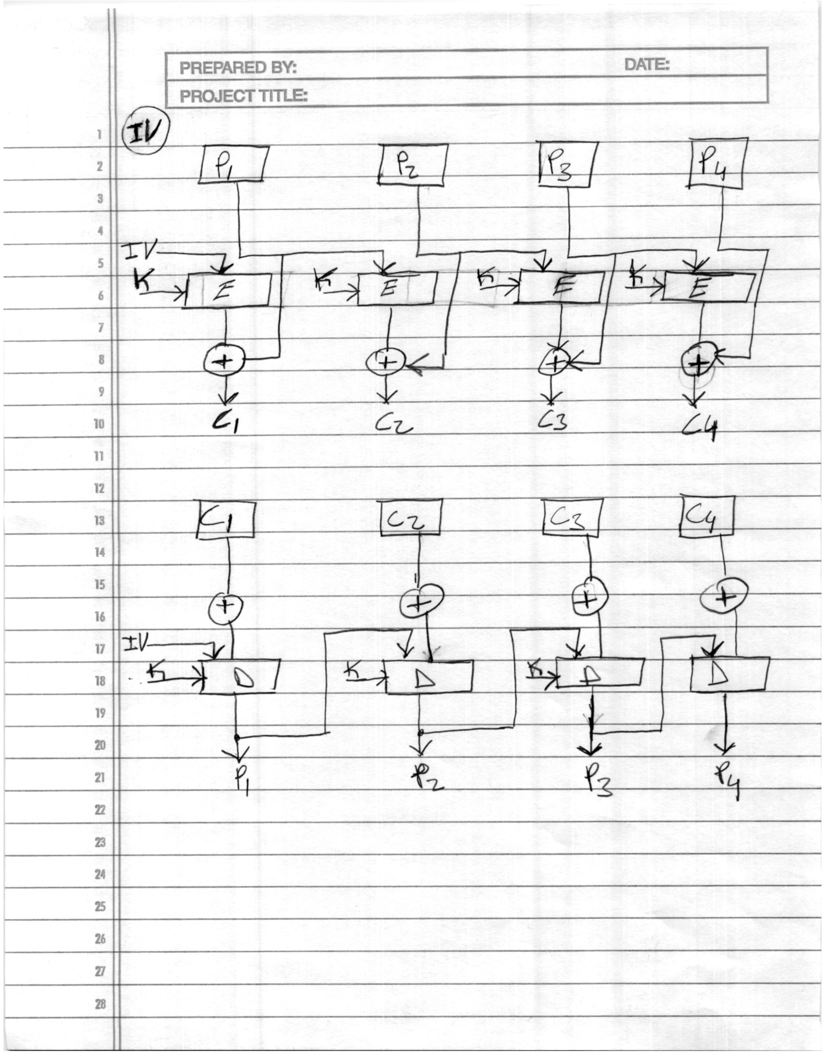


Figure 1: Encryption Procedures

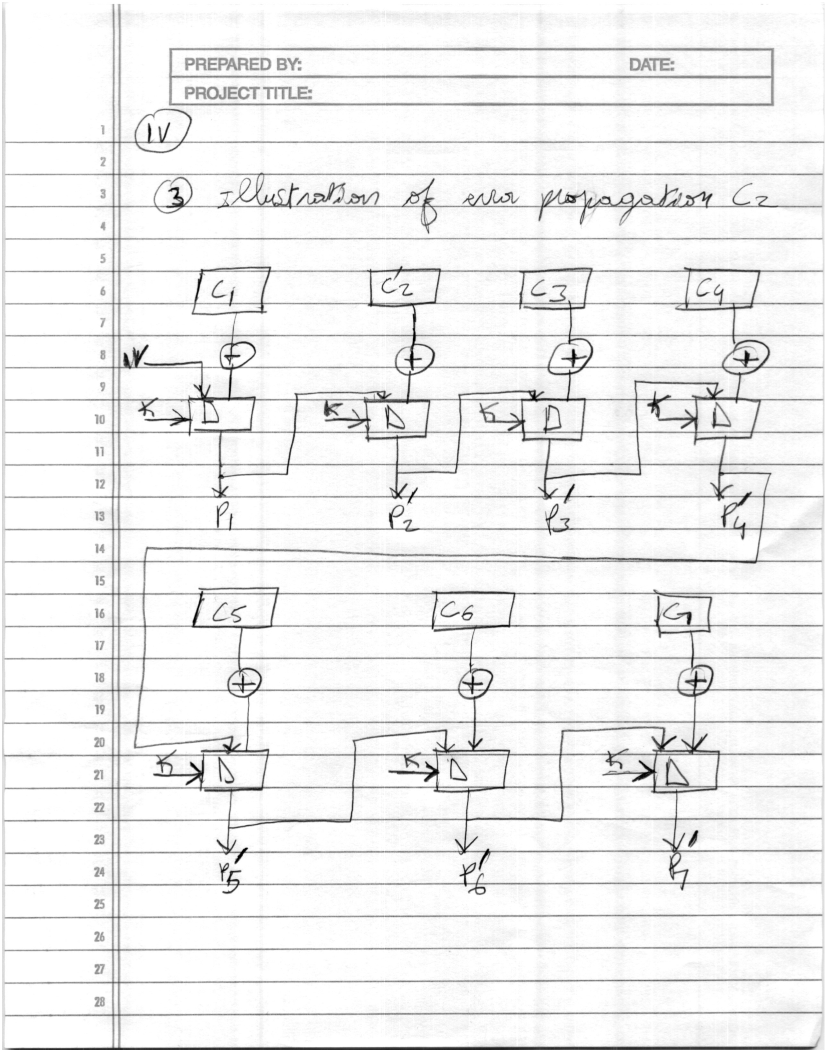
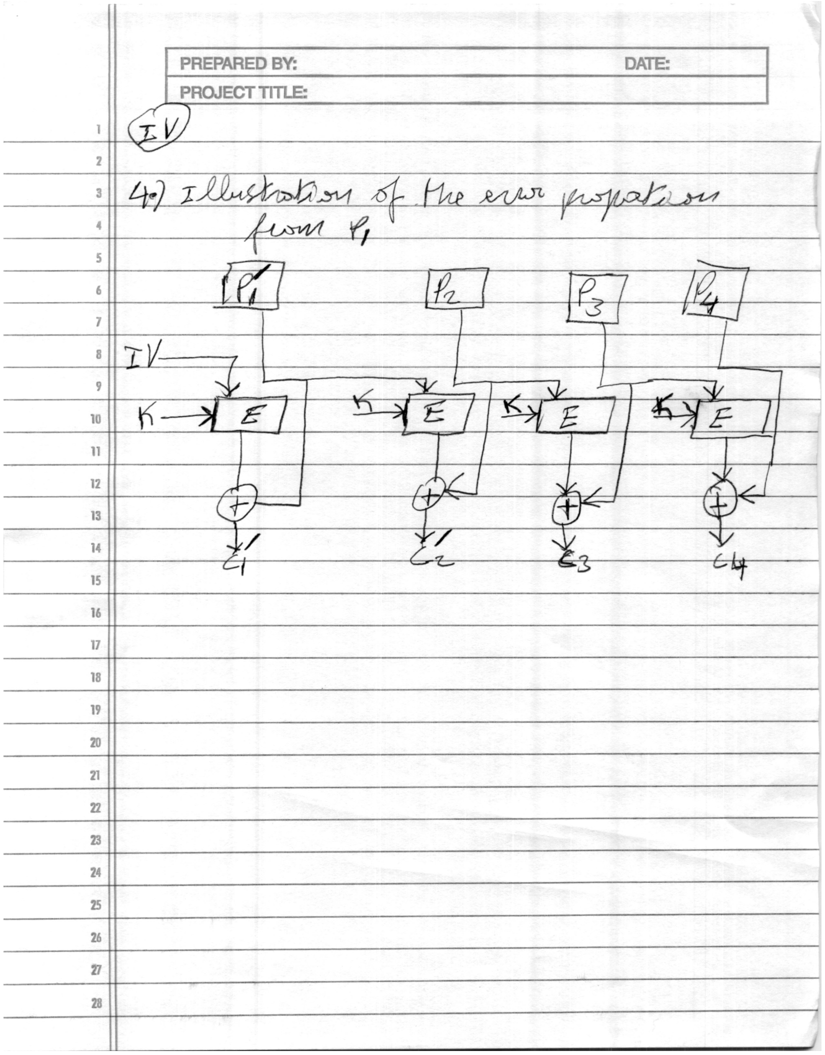


Figure 2: Illustration of Error Propagation from C_2



PREPARED BY: DATE:

PROJECT TITLE:

IV

4) Illustration of the error propagation from P_1

Figure 3: Illustration of the Error Propagation from P_1

3. If an error happened to C_2 during the transmission (all other blocks are transmitted correctly), which blocks of plaintext could not recovered at the receiver? Please explain.

   Observing $Figure2$ if C_2 is corrupted, the error would get progated accross the successor block chains because the outputs of the predecessors that were corrupted would are used the successors blocks. As a result, the error would keep propagation accross the chains.

4. If an error happened to P_1 before encryption, through how many blocks are of ciphertext is the error propagated? Which blocks of plaitext could not be recovered at the receiver? Please explain.

   With the observation of the block chaining structure in $Figure3$, we could see that only C_1 and C_2 would be affected by the error.

   Let perform a demonstration to understand the block that could be recovered:

   $P_i = C_i \oplus D_k(P_{i-1})$
   $P_i = E_k(P_{i-1}) \oplus P_i \oplus D_k(P_{i-1})$
   $P_1' = E_k(P_0) \oplus P_1' \oplus D_k(P_0)$
   $P_1' = P_1'$

   Now We could try to apply the same logic to another block. Let use P_2':

   $P_i = C_i \oplus D_k(P_{i-1})$
   $P_i = E_k(P_{i-1}) \oplus P_i \oplus D_k(P_{i-1})$
   $P_2' = E_k(P_1') \oplus P_2 \oplus D_k(P_1')$
   $P_2' = P_2$

   We could see that P_2 could be recovered and P_1 is not going to be recovered.

5. Is this a good block cipher operation mode in your opinion? Justify your answer.

   This design could be usable because the error propagation can be reduced to certain number of blocks. For instance, we have seen that an error from a encryption block can only affect the block itself and its successor in chain instead of propagating in the entire chain. Also, we have seen that with a set of corrupted plaintext. Some of the plaintext could be recovered according the formula we have used. Therefore, this chaining could be used data transmission because in case an error happened during the transmission, the likelihood of recovering the original information could be possible because of the features we have previously described.

5 RSA Algorithm Analysis

1. Explain how does the decryption operation recover the plaintext?

First, the RSA alogrithm is practical because of the Eurler's Theorem:

We have for any integer (message) relatively prime to n,
$M^{\phi(n)} = 1(\mod n)$

We know that $\phi(n)$ is the Euler totient function:
$\phi(n) = \phi(p).\phi(q)$
$= (p-1)(q-1)$
$= n - (p+q) + 1$

Since the private key d is relatively prime to $\phi(n)$, it would have a multiplicative inverse public key e of the modulo of $\phi(n)$:

$e.d = 1(\mod \phi(n))$

If e and d are correctly choosen we could have the following equation:
$D(E(M)) \equiv (E(M))^d \equiv (M^e)^d(\mod n) = M^{e.d}(\mod n)$

and also

$M^{e.d} \equiv M^{k.\phi(n)+1} \mod n$

From the above equation we could write the following equation:

$(M^{\phi(n)} \mod n)^k.M \mod n$

We know that $(M^{\phi(n)})^k = 1$ according to the Euler theorem. Therefore we could write:

$M \mod n = M$ for all M, $0 \leq M < n$.

Why value of the plaintext M must be less n?

The value of M must be less than n because of the following reason:

Let suppose that one of the primes, for instance q divides M. Therefore, $M \equiv 0(\mod q)$ and we have $0 \equiv M^{1+k\phi(n)} \equiv m(\mod q)$.
As a result, q could divide M, but p cannot divide M since $n = pq$ so that we could have $gcd(M, p) = 1$. As a result, $M < n$ to maintain these properties.

2. Suppose that A is quite longer than n (for example, n is about 400 digits long, but M is 5,000 digit long). Please propose a scheme to encrypt M so that B could recover M using B's private key.

   Let e_B and d_B be B's public and private keys respectively. We would use the following illustration for the encryption and decryption of M

$M^{e_B} \mod n = C$

To decrypt C, we would have to discover the private of B with the following equation.

$e_B.d_B = \phi(n)k + 1$
$d_B = \frac{\phi(n)k+1}{e_B}$
$M = C^{\frac{\phi(n)k+1}{e_B}} \mod n$
$M = C^{d_B} \mod n$

Since in this case, $M > n$ it could be infeasible to recover M.

6 Short answer questions

1. Please list the main causes of cloud security problems.

   The following are the causes of cloud security problems.

   (a) Loss of control

   (b) Lack of trust (mechanisms)

   (c) Multi-tenancy

2. If A is to send a confidential message to B using public cryptography, what kind of key A use?

   In this situation, A should use the public of B.

3. If A is to send a piece of message to B so that B can autenticate that this message is from A, what kind of key should A use?

   In this situation, the private key A would be used.

4. What is avalanche effect in a cipher? Is this a good property or not? Please explain your answer.

   The avalanche effect is desirable property of encryption algorithm where a change of *one* input or key bit results in changing $half$ output bits. We believe that it is good property because it would a change made in the plaintext or ciphertext cannot deduce by the cryptanalyst because the ouput would be extremely different.

5. Why are modern ciphers designed as product ciphers instead of pure substitution ciphers?

   Modern ciphers are designed as product ciphers to be more resistant to exhaustive-search attack because it is the combinaison of different components such as diffusion and confusion. Also, modern ciphers are made of different combinations such as transposition units (P-boxes) and substitution units (S-boxes) to give more security. For instance, the S-box is designed to be resistant to known cryptanalytic attack because the Rijndael developers sought a design that has a low correlation between input bits and outputs bits, and the property that the output cannot be described as a simple mathematical function of the input

7 Reference

Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, A method for obtaining digital signatures and public key signatures, Communications of the ACM, Vol. 21, No. 2, Feb. 1978; or reprinted in Secure Communications and Assymmetric Cryptosystems, AAAS Selected Synposium 69, Westview Press, Boulder, CO, 1982