University of New Brunswick, Faculty of Computer Science

CS4355/6355: Topic 1 – Additional Note

1 Simple Substitution Ciphers

As Julius Caesar surveys the unfolding battle from his hilltop outpost, an exhausted and disheveled courier bursts into his presence and hands him a sheet of parchment containing gibberish:

j s j r d k f q q n s l g f h p g w j f p y m w t z l m n r r n s j s y q z h n z x

Within moments, Julius sends an order for a reserve unit of charioteers to speed around the left flank and exploit a momentary gap in the opponentŠs formation.
How did this string of seemingly random letters convey such important information?

Please use the simple substitution cipher: $ciphertext = plaintext + key \mod 26$ to recover the plaintext of the string and the used key, and explain why.

University of New Brunswick, Faculty of Computer Science

CS4355/6355: Topic 2 – Additional Note

1 DES and AES Problems

1. Let K be a 56-bit DES key, and let M be a 64-bit plaintext, given the ciphertext

$$C = DES(K, M) \tag{1.1}$$

how to recover the key K and the plaintext M?

Solutions.

- Case 1: If M is meaningless, e.g., password, secret key, we cannot verify whether a key is correct or not.
- Case 2: If M is meaningful,
  - For each key $k \in \{0,1\}^{56}$ do
  - $\quad M = DES^{-1}(k, C)$
  - $\quad$ if M is meaningful, return $k||M$

2. Let K be a 56-bit DES key, let L be a 64-bit string, and let M be a 64-bit plaintext, check the following two algorithms derived from DES are secure or not.

$$case\ 1: \quad C = DES(K, L \oplus M) \tag{1.2}$$

$$case\ 2: \quad C = L \oplus DES(K, M) \tag{1.3}$$

For each algorithm, three pairs of plaintext-ciphertext $(M_1, C_1), (M_2, C_2), (M_3, C_3)$ are available for your cryptanalysis.

Solutions.

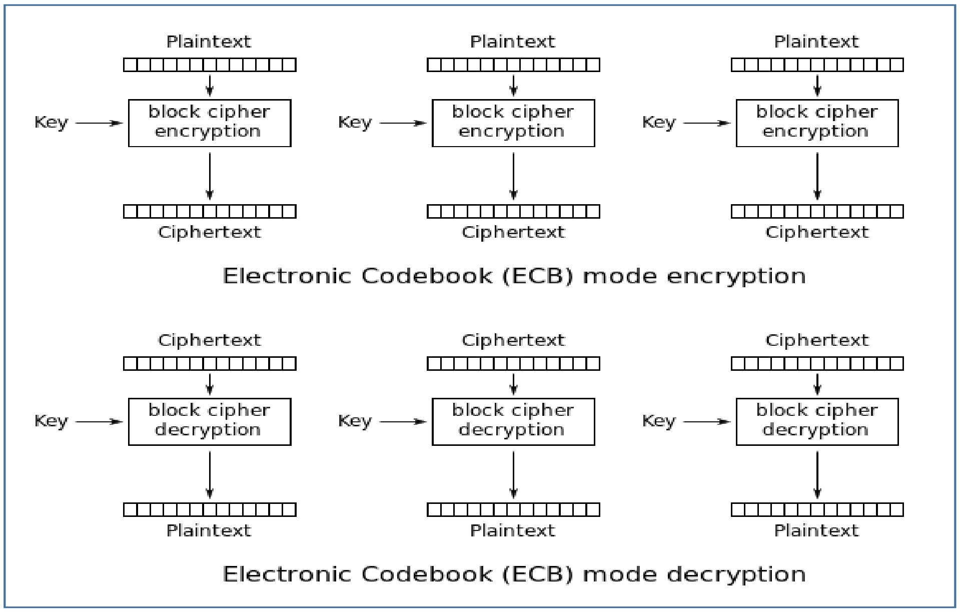
- Case 1
  - For each key $k \in \{0,1\}^{56}$ do
  - $L_1 = DES^{-1}(k, C_1) \oplus M_1$, $L_2 = DES^{-1}(k, C_2) \oplus M_2$, and $L_3 = DES^{-1}(k, C_3) \oplus M_3$
  - if $L_1 = L_2 = L_3$, return $k || L_1$
- Case 2
  - For each key $k \in \{0,1\}^{56}$ do
  - $L_1 = DES(k, M_1) \oplus C_1$, $L_2 = DES(k, M_2) \oplus C_2$, and $L_3 = DES(k, M_3) \oplus C_3$
  - if $L_1 = L_2 = L_3$, return $k || L_1$

3. Assume AES is a secure PRF (Pseudorandom Function), define a function $F(K, M) = AES(M, K)$. Is $F(K, M)$ is a secure PRF?

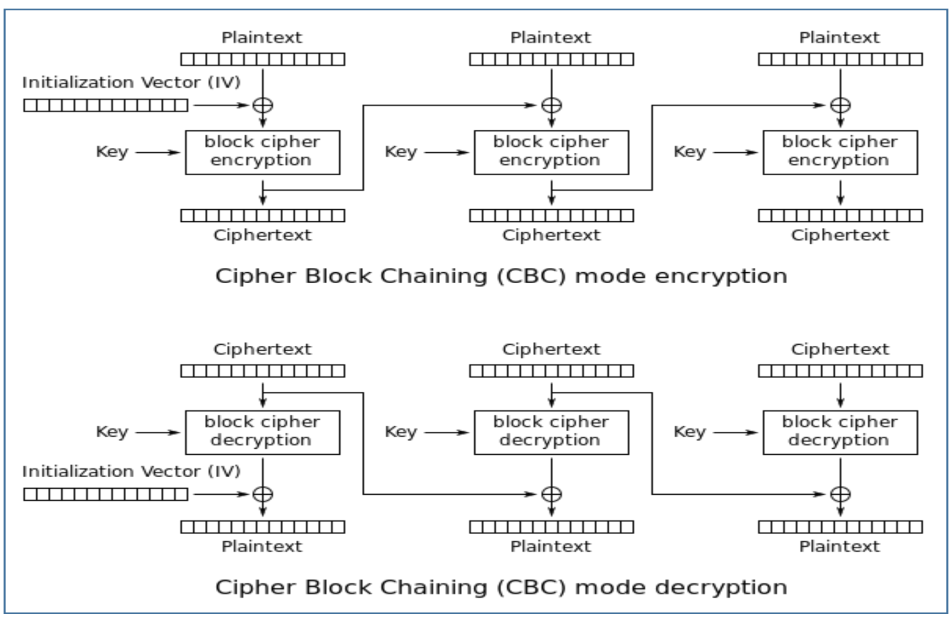
   Solution. Once we are given a pair of plaintext-ciphertext (M, C), we can easily recover the key K as $AES^{-1}(M, C) = K$. Thus, $F(K, M)$ is not a secure PRF.

2 Block Cipher Modes

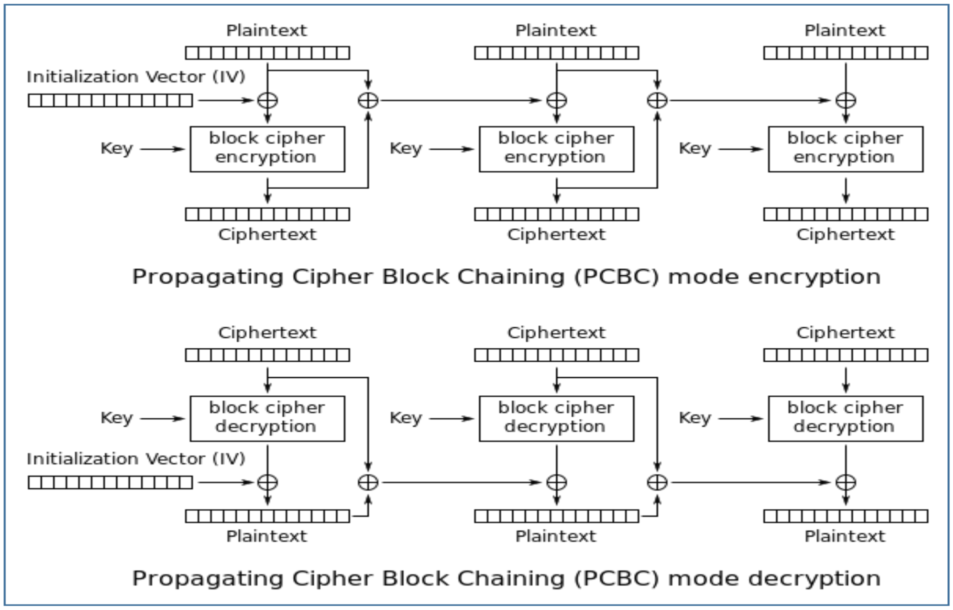
- Electronic Codebook (ECB)



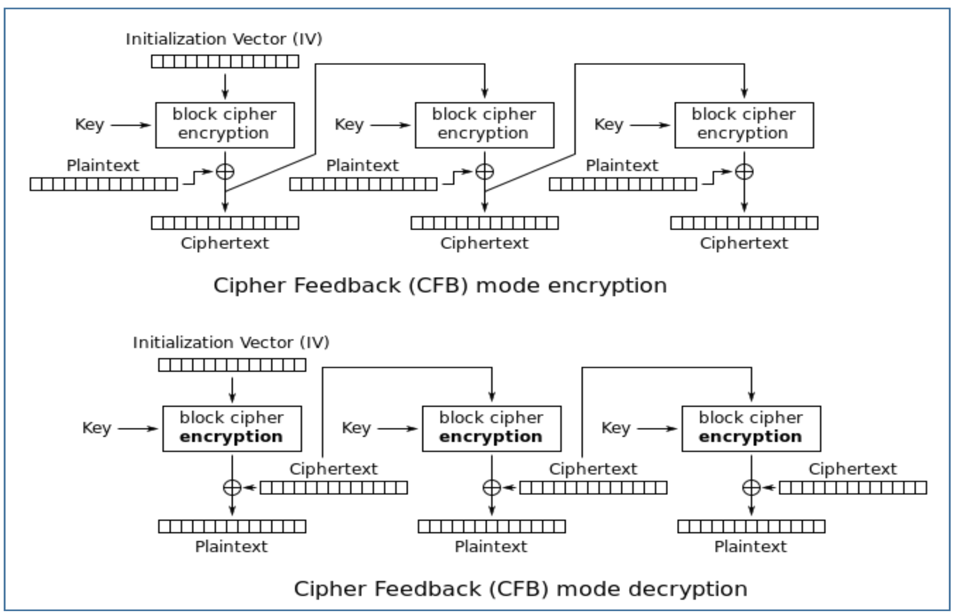
- Cipher Block Chaining (CBC)



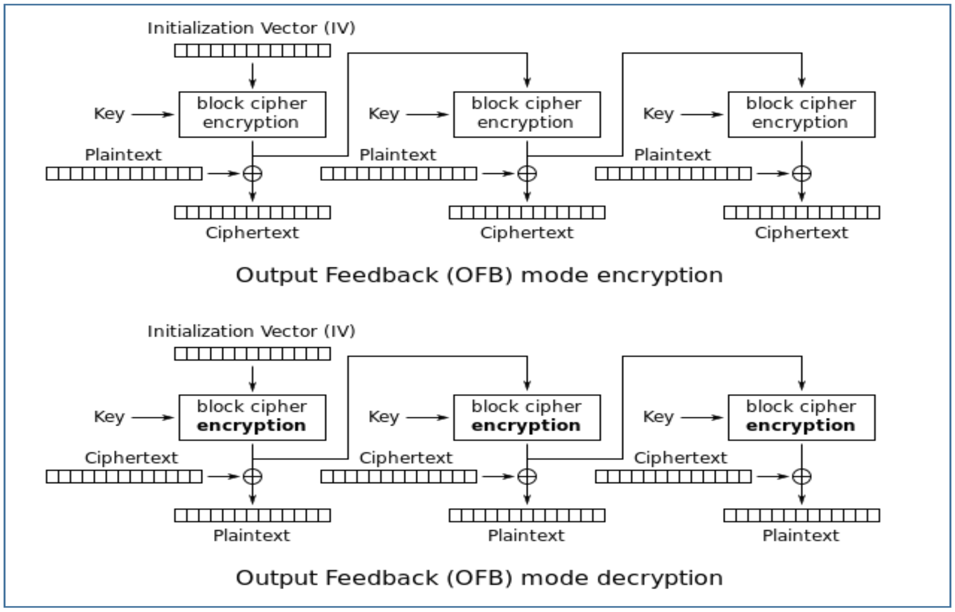
- Propagating Cipher Block Chaining (PCBC)



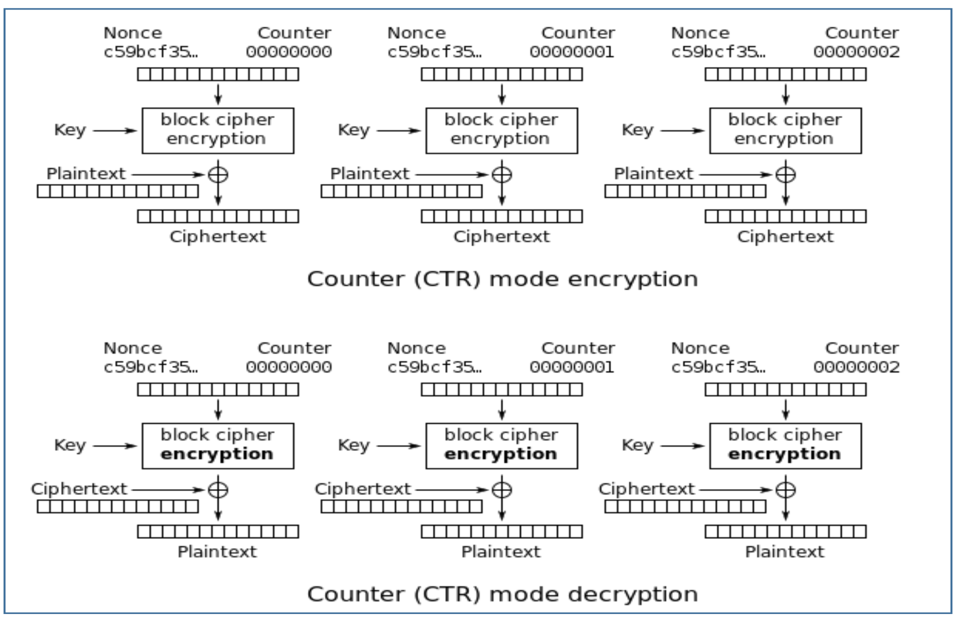
- Cipher Feedback (CFB)



- Output Feedback (OFB)


Initialization Vector (IV)
Key
block cipher encryption
Plaintext
Ciphertext
Output Feedback (OFB) mode encryption
Initialization Vector (IV)
Key
block cipher encryption
Ciphertext
Plaintext
Output Feedback (OFB) mode decryption

- Counter (CTR)


Nonce
c59bcf35...
Counter
00000000
00000001
00000002
Key
block cipher encryption
Plaintext
Ciphertext
Counter (CTR) mode encryption
Nonce
c59bcf35...
Counter
00000000
00000001
00000002
Key
block cipher encryption
Ciphertext
Plaintext
Counter (CTR) mode decryption

University of New Brunswick, Faculty of Computer Science

CS4355/6355: Topic 2 – Additional Note

1 Group Problems

Check whether the following sets can form group under the given operation?

- Case 1: the set of real numbers R, for the operation $a \circ b = 2(a+b)$

  Answer: Cannot. Because for the given operation $a \circ b = 2(a+b)$, there is no identity. Suppose x is the identity, we have $x \circ 0 = 2(x+0) = 2x = 0$, thus $x = 0$. However, for 1, $1 \circ 0 = 2(1+0) = 2 \neq 1$, which is contradictory to $x = 0$.

- Case 2: $G = \{1, -1\}$, for the ordinary multiplication operation.

  Answer: Can.

$\times$	1	-1
1	1	-1
-1	-1	1

- Case 3: Non-Zero Real Number Set R^*, for operation $a \circ b = 2ab$.

  Answer: Can. It is easy to see Associativity is satisfied; 1/2 is the identity of R^*, for any $a \in R^*$, $\frac{1}{4a}$ is its inverse.

- Case 4: Let $G = \{(a,b)|a, b$ are real numbers and $a \neq 0\}$, for the operation $(a,b) \circ (c,d) = (ac, ad+b)$.

  Answer: Can. Check the followings:

  - G is a non-empty set

- Closure: for any (a, b), (c, d) in G, where $a \neq 0, c \neq 0$, we have $(ac, ad + b)$ are still real numbers and $ac \neq 0$, thus $(a, b) \circ (c, d) = (ac, ad + b)$ is still in G.
- Associativity: (e, f) in G, we have

$$[(a, b) \circ (c, d)] \circ (e, f) = (ac, ad + b) \circ (e, f) = (ace, acf + ad + b)$$

$$(a, b) \circ [(c, d) \circ (e, f)] = (a, b) \circ (ce, cf + d) = (ace, acf + ad + b)$$

- Existence of Identity: $(1, 0)$ in G, and $(1, 0) \circ (a, b) = (a, b)$, i.e., $(1, 0)$ is the left identity. (it is easy to see $(1, 0)$ is the right identity)
- Existence of Inverse: (a, b) in G, we have $(1/a, -b/a)$ in G and $(1/a, -b/a) \circ (a, b) = (1, 0)$ (it is easy to see $(1/a, -b/a)$ is the right identity)
- Therefore, it is a group. But it is not a commutative group, for example

$$(3, 6) = (1, 2) \circ (3, 4) \neq (3, 4) \circ (1, 2) = (3, 10)$$

University of New Brunswick, Faculty of Computer Science

CS4355/6355: Topic 3 – Additional Note

1 Group Problems

1. Let G be a group. Please prove G is an abelian group if and only if for any elements $a, b \in G$, the condition $(ab)^2 = a^2b^2$ is true.

   Proof. (1) If G is an abelian group, then for any elements $a, b \in G$, we have $(ab)^2 = (ab)(ab) = a^2b^2$.

   (2) For any elements $a, b \in G$, we have $(ab)^2 = a^2b^2$, that is, $abab = aabb$. Both sides left-multiplies a^{-1}, right-multiplies b^{-1}, we have

   $$a^{-1}ababb^{-1} = a^{-1}aabbb^{-1} \Rightarrow ebae = eabe \Rightarrow ba = ab$$

   As a result, it is an abelian group.

2. Let G be a group, and a, b, c are any three elements in G. Please prove the equation $xaxba = xbc$ has *one and only one* solution in G.

   Proof.

   $$xaxba = xbc \Rightarrow x^{-1}xaxba = x^{-1}xbc \Rightarrow axba = bc \Rightarrow a^{-1}axba = a^{-1}bc \Rightarrow xba = a^{-1}bc$$
   $$\Rightarrow xbaa^{-1} = a^{-1}bca^{-1} \Rightarrow xb = a^{-1}bca^{-1} \Rightarrow xbb^{-1} = a^{-1}bca^{-1}b^{-1}$$
   $$\Rightarrow x = a^{-1}bca^{-1}b^{-1}$$

   Therefore, it is easy to see $x = a^{-1}bca^{-1}b^{-1}$ is one solution for the equation $xaxba = xbc$.

Assume y is another solution of the equation

$$xaxba = xbc \tag{1.1}$$

i.e., we have

$$yayba = ybc \tag{1.2}$$

From Eq.(1.1), we have

$$axbac^{-1}b^{-1} = e$$

From Eq.(1.2), we have

$$aybac^{-1}b^{-1} = e$$

As a result, $x = y$. That is, the equation $xaxba = xbc$ has *one and only one* solution in G.

3. Let G be a group, please prove the elements within each case have the same order.

   - Case 1: a and a^{-1}.

     Proof. Assume $a^n = e$, we have

     $$(a^{-1})^n = a^{-n} = (a^n)^{-1} = e^{-1} = e$$

     that is, $(a^{-1})^n = e$. On the other hand, assume $(a^{-1})^n = e$, we have

     $$a^n(a^{-1})^n = a^n a^{-n} = e.$$

     we have $a^n = e$. Therefore, $|a| = |a^{-1}|$. (Note $|a|$ denotes the order of a.)

     Proof 2. We always have $aa^{-1} = e$, we have $aaa^{-1}a^{-1} = aea^{-1} = e$. Continue it, we have

     $$a^n(a^{-1})^n = e$$

     if $a^n = e$, we have $(a^{-1})^n = e$, and vice verse.

   - Case 2: a and cac^{-1} for any $c \in G$.

     Proof. Assume $a^n = e$, we have $ca^nc^{-1} = cec^{-1} = e$. Then,

     $$\underbrace{cac^{-1}cac^{-1}\cdots cac^{-1}}_{n} = ca^nc^{-1} = e$$

     We have $(cac^{-1})^n = e$.

     On the other hand, if $(cac^{-1})^n = e$, we have

     $$e = (cac^{-1})^n = \underbrace{cac^{-1}cac^{-1}\cdots cac^{-1}}_{n} = ca^nc^{-1}$$

     Then, $c^{-1}ca^nc^{-1}c = c^{-1}ec \Rightarrow a^n = e$. Therefore, $|a| = |cac^{-1}|$.

- Case 3: ab and ba.

  Proof. Assume $(ab)^n = e$, that is,

$$(ab)^n = \underbrace{(ab)(ab)\cdots(ab)}_{n} = e \Rightarrow a^{-1}\underbrace{(ab)(ab)\cdots(ab)}_{n}b^{-1} = a^{-1}eb^{-1}$$

$$\Rightarrow \underbrace{(ba)(ba)\cdots(ba)}_{n-1} = a^{-1}eb^{-1} \Rightarrow \underbrace{(ba)(ba)\cdots(ba)(ba)}_{n} = a^{-1}eb^{-1}(ba) = e$$

  Therefore, $(ba)^n = e$, and vice versa. Therefore, $|ab| = |ba|$.

  Proof 2. Use the result of Case 2. Because

$$ab = a(ba)a^{-1}$$

  from the result of Case 2, we have $|ab| = |ba|$.

- Case 4: abc, bca, cab.

  Proof. Use the result of Case 2. Because

$$bca = a^{-1}(abc)a, \quad cab = c(abc)c^{-1}$$

  from the result of Case 2, we have $|abc| = |bca| = |cab|$.

4. Let G be a group, and an element $a \in G$ has the order n. Please prove $a^s = a^t \Leftrightarrow n|(s-t)$.

   Proof. Because $a^s = a^t$, we have

$$a^s = a^t \Rightarrow a^s(a^{-t}) = a^t a^{-t} = e \Rightarrow a^{s-t} = e$$

   Therefore, $n|(s-t)$.

   On the other side, $n|(s-t) \Rightarrow (s-t) = n \cdot k$ for some k. Then, $a^{s-t} = a^{n \cdot k} = e$.

$$a^{s-t} = e \Rightarrow a^{s-t}a^t = ea^t \Rightarrow a^s = a^t$$

2 Ring Problem

1. Let R be a ring with identity (denoted as 1). Prove R is also a ring with the identity under the operations $a \oplus b = a + b - 1$, $a \circ b = a + b - ab$.

   Proof.

   Under $\oplus$, R is a group. We easily check it is non-empty, closure, identity $=1$, and a's inverse is $2 - a$.

   Regarding Associativity,

$$(a \oplus b) \oplus c = a \oplus (b \oplus c) = a + b + c - 2$$

Under $\circ$, Associativity

$$(a \circ b) \circ c = a \circ (b \circ c) = a + b + c - ab - ac - bc + abc$$

Also,

$$a \circ (b \oplus c) = (a \circ b) \oplus (a \circ c) = 2a + b + c - 1 - ab - ac$$

Similarly,

$$(a \oplus b) \circ c = (a \circ c) \oplus (b \circ c)$$

As a result, R for the operations $(\oplus, \circ)$ is a ring.

University of New Brunswick, Faculty of Computer Science

CS4355/6355: Topic 3 – Additional Note

1 Number Theory Problems

1. Let n be an integer than 1. Prove that 2^n is the sum of two odd consecutive integers.

   Proof. For the problem, the relation $2^n = (2k-1) + (2k+1)$ implies $k = 2^{n-2}$ and we obtain $2^n = (2^{n-1} - 1) + (2^{n-1} + 1)$.

   $\square$

2. Let n be an integer than 1. Prove that 3^n is the sum of three consecutive integers.

   Proof. For this problem, the relation $3^n = (s-1) + s + (s+1)$ implies $s = 3^{n-1}$ and we obtain the representation $3^n = (3^{n-1} - 1) + 3^{n-1} + (3^{n-1} + 1)$.

   $\square$

3. Prove that if x, y, z are integers such that $x^2 + y^2 = z^2$, then $xyz \equiv 0 \bmod 30$.

   Proof.

   - First, all three of x, y, z cannot be odd, since odd + odd = even. So xyz is even, i.e., $2|(xyz)$.
   - Second, $1^2 \equiv 2^2 \equiv 1 \bmod 3$, all perfect squares are 0 or 1 mod3. However, $x^2 + y^2 \equiv z^2 \bmod 3$ is not solved by making each of x^2, y^2, z^2 be 1 mod 3. Thus, one is 0 mod 3, and so xyz is divisible by 3, i.e., $3|(xyz)$

- Third, we have $1^2 \equiv 4^2 \equiv 1 \bmod 5$, and $2^2 \equiv 3^2 \equiv -1 \bmod 5$. So $x^2 + y^2 = z^2 \bmod 5$ can look like:

$$left\ side = \begin{cases} case1: & 1+1 = 2 \bmod 5 \\ case2: & 1+(-1) = 0 \bmod 5 \\ case3: & (-1)+1 = 0 \bmod 5 \\ case4: & (-1)+(-1) = -2 = 3 \bmod 5 \end{cases}$$

$$right\ side = \begin{cases} case1: & 1 \bmod 5 \\ case2: & -1 \bmod 5 \end{cases}$$

  If none of x, y, z is $0 \bmod 5$, the left side is NOT equal to the right side. Therefore, one of x, y, z is $0 \bmod 5$, and xyz is divisible by 5, i.e., $5|(xyz)$.

  Finally, because $2|(xyz)$, $3|(xyz)$, and $5|(xyz)$, we have $2 \cdot 3 \cdot 5|(xyz)$, i.e., $xyz \equiv 0 \bmod 30$.

$\square$

CS4355/6355: Topic 3 – Additional Note

1 Number Theory Problems

1. If $p|10a-b$, $p|10c-d$, then $p|ad-bc$.

   Proof. From $p|10a-b$, we know $p \cdot k_1 = 10a-b$ for some k_1. Then,

   $$p \cdot k_1 \cdot c = (10a-b) \cdot c$$

   Let $k_2 = k_1 \cdot c$, we have $p \cdot k_2 = (10a-b) \cdot c = 10ac - bc$.
   Similarly, we have $p \cdot k_4 = (10c-d) \cdot a = 10ca - ad$ for some k_4. Then,

   $$p \cdot k_2 - p \cdot k_4 = 10ac - bc - 10ac + ad \Rightarrow p(k_2-k_4) = ad - bc$$

   Therefore,

   $$p|ad-bc$$

   □

2. If n is odd, then $3|2^n+1$

   Proof. Since $2+1 \equiv 0 \bmod 3$, we have $2 \equiv -1 \bmod 3$. Then,

   $$2^n \equiv (-1)^n \bmod 3$$

   Because n is odd, we have

   $$2^n - (-1)^n \equiv 0 \bmod 3 \Rightarrow 2^n + 1 \equiv 0 \bmod 3 \Rightarrow 3|2^n+1$$

   □

3. $k = 0, 1, 2, \cdots$, for $n \in \mathbb{Z}$, we have $2n+1 | 1^{2k+1} + 2^{2k+1} + \cdots + (2n-1)^{2k+1} + 2n^{2k+1}$.

Proof. For each $i = 1, 2, \cdots, n$, we have

$$i + (2n+1) - i \equiv 2n+1 \equiv 0 \bmod 2n+1$$

$$i \equiv -((2n+1)-i) \bmod 2n+1 \Rightarrow i^{2k+1} \equiv [-((2n+1)-i)]^{2k+1} \bmod 2n+1$$

Since $2k+1$ is odd, we have

$$i^{2k+1} + ((2n+1)-i)^{2k+1} \equiv 0 \bmod 2n+1$$

$$\sum_{i=1}^{n} [i^{2k+1} + ((2n+1)-i)^{2k+1}] \equiv 0 \bmod 2n+1$$

Therefore,

$$2n+1 | 1^{2k+1} + 2^{2k+1} + \cdots + (2n-1)^{2k+1} + 2n^{2k+1}$$

□

4. If $m-p | mn+pq$, then $m-p | mq+np$

Proof. Since

$$(m-p)|(m-p)(n-q) \Rightarrow (m-p)|mn+pq-(mq+np)$$

Because $m-p|mn+pq$, we have $m-p|mq+np$. □

5. If $x \equiv 1 \bmod m^k$, then $x^m \equiv 1 \bmod m^{k+1}$.

Proof. Since $x \equiv 1 \bmod m^k$, we have $x = 1 + k \cdot m^k = 1 + (k \cdot m^{k-1}) \cdot m$, thus

$$m^k | x-1, \qquad x \equiv 1 \bmod m$$

From $x \equiv 1 \bmod m$, we have $x^i \equiv 1^i \bmod m$ for $i = 0, 1, \cdots m-1$. Then,

$$\sum_{i=0}^{m-1} x^i \equiv \sum_{i=0}^{m-1} 1^i \bmod m$$

$$1 + x + x^2 + \cdots + x^{m-1} \equiv m \bmod m \Rightarrow 1 + x + x^2 + \cdots + x^{m-1} \equiv 0 \bmod m$$

Then,

$$m | (1 + x + x^2 + \cdots + x^{m-1})$$

Finally, we have

$$m^k \cdot m | (x-1)(1 + x + x^2 + \cdots + x^{m-1}) \Rightarrow m^{k+1} | x^m - 1 \Rightarrow x^m \equiv 1 \bmod m^{k+1}.$$

□

UNIVERSITY OF NEW BRUNSWICK, FACULTY OF COMPUTER SCIENCE

CS4355/6355: Topic 3 – Additional Note

1 Number Theory Problems

1. Let n be a positive integer. Prove that $3^{2^n} + 1$ is divisible by 2, but not by 4.

   Proof. **Method 1.** Clearly, 3^{2^n} is odd and $3^{2^n} + 1$ is even. Note that $3^{2^n} = (3^2)^{2^{n-1}} = 9^{2^{n-1}} = (8+1)^{2^{n-1}}$. Recall the **Binomial theorem**

   $$(x+y)^m = x^m + \binom{m}{1}x^{m-1}y + \binom{m}{2}x^{m-2}y^2 + \cdots + \binom{m}{m-1}xy^{m-1} + y^m$$

   Setting $x = 8, y = 1$, and $m = 2^{n-1}$ in the above equation, we see that each summand besides the last (that is, $y^m = 1$) is a multiple of 8 (which is a multiple of 4). Hence the remainder of 3^{2^n} on dividing by 4 is equal to 1, and the remainder of $3^{2^n} + 1$ on dividing by 4 is equal to 2. □

   Proof. **Method 2.** We have $3 + 1 \equiv 0 \bmod 4$, that is, $3 \equiv -1 \bmod 4$. Then, $3^{2^n} \equiv (-1)^{2^n} \bmod 4$, we have $3^{2^n} \equiv 1 \bmod 4$. As a result, $3^{2^n} + 1 \equiv 2 \bmod 4$, the proof is completed.

   □

2. Let p be a prime number. Then $x^2 \equiv 1 \bmod p$ if and only if $x \equiv \pm 1 \bmod p$.

   Proof. If $x \equiv \pm 1 \bmod p$, we have $x^2 \equiv 1 \bmod p$. Conversely, if $x^2 \equiv 1 \bmod p$, then p divides $x^2 - 1 = (x-1)(x+1)$, and so p must divide $x - 1$ or $x + 1$. □

3. If p is prime, then $(p-1)! \equiv -1 \bmod p$.

Proof. If $p = 2$, $(p-1)! \equiv -1 \bmod p$ is true, since $1! \equiv -1 \bmod 2$.

If $p = 3$, $(p-1)! \equiv -1 \bmod p$ is also true, since $2! \equiv -1 \bmod 3$.

If p is prime ≥ 5, we know $(Z_p^*, *)$ is a group, where $Z_p^* = \{1, 2, 3, \cdots, p-1\}$ has total $p-1$ elements. Based on the Group theory, each element $a \in Z_p^*$ has its inverse $a^{-1} \in Z_p^*$ such that $a * a^{-1} \equiv 1 \bmod p$. Based on the Question 2 above, we know $a = a^{-1}$ if and only $a = 1$ or $a = p-1$. Therefore, we can partition the $p-3$ numbers in the set $\{2, 3, \cdots, p-2\}$ into $(p-3)/2$ pairs of integers $\{a_i, a_i^{-1}\}$ such that $a_i * a_i{}^{-1} \equiv 1 \bmod p$ for $i = 1, 2, \cdots, (p-3)/2$. Then,

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \equiv (p-1) \prod_{i=1}^{(p-3)/2} a_i a_i^{-1} \equiv p-1 \equiv -1 \bmod p.$$

□

4. Let $p \geq 7$ be a prime. Prove that the number

$$\underbrace{11 \cdots 1}_{p-1 \quad 1's}$$

is divisible by p.

Proof. We have

$$\underbrace{11 \cdots 1}_{p-1 \quad 1's} = \frac{10^{p-1} - 1}{9}$$

and the conclusion follows from Fermat's Little Theorem. (Note also that $\gcd(10, p) = 1$.) □

UNIVERSITY OF NEW BRUNSWICK, FACULTY OF COMPUTER SCIENCE

CS4355/6355: Topic 4 – Additional Note

---

1 The cycling attack

The cycling attack was one of the first attacks on RSA [1]. As the name of this attack suggests, the way this attack works is by repeatedly encrypting the ciphertext. When an attacker gets $c \equiv m^e \bmod n$, he will encrypt the ciphertext with the public key and this will lead him to, eventually getting an encryption which will be the original ciphertext. That is, after l encryptions, he will have

$$c^{e^l} \equiv c \equiv m^e \bmod n$$

so he will know that the previous encryption is the original plaintext, that is,

$$c^{e^{l-1}} \equiv m \bmod n$$

The value l is called the recovery exponent for the plaintext m. Suppose a plaintext m is encrypted with the public key (e, n), the recovery exponent of m divides $\phi(\phi(n))$. Because $e \in Z^*_{\phi(n)}$, we have $e^{\phi(\phi(n))} \equiv 1 \bmod n$. If $ord(e) = l$, we have $l | \phi(\phi(n))$. We need to choose e with a larger l.

2 Pollard's ρ algorithm

Pollard's ρ algorithm, described by Pollard in 1975 [2], is to find a small factor p of a given integer N. The simplified version of this algorithm is described as follows.
Algorithm: Pollard's ρ Algorithm: Given a composite $N = pq$:

1. set $a = 2, b = 2$.
2. Define the modular polynomial $f(x) = (x^2 + c) \bmod N$, with $c \neq 0, -2$
3. For $i = 1, 2, \cdots$ do:
   a) Compute $a = f(a), b = f(f(b))$.
   b) Compute $d = (a - b, N)$.
   c) If $1 < d < N$, then return d with success.
   d) If $d = N$, then terminate the algorithm with failure.

The function f is used to create two pseudo random sequences on $\mathbb{Z}_N$. The reason for this is that, picking randomly two numbers $x, y \in \mathbb{Z}_N$, there is a probability of 0.5 that after $1.777\sqrt{p}$ tries, one will be congruent modulo p. If they are $a \neq b$, then $(a - b, N)$ yields a factor of N [3]. Concretely,

$$a, b \in \mathbb{Z}_N \to a' = a \bmod p, b' = b \bmod p \to a', b' \in \mathbb{Z}_p^*$$

After $1.777\sqrt{p}$ tries, we may have $a' = b' \bmod p$, which also shows $a = b \bmod p$. Then, we have $p|(a - b)$, and $\gcd(a - b, N) = p$.
The runtime of the algorithm is $O(\sqrt{p})$, where p is N's smallest prime factor [4]. This means that against an RSA modulus N with balanced primes the runtime of the algorithm is $O(N^{1/4})$, making its an inefficient method.

Example.
Let $N = 8051$ and $f(x) = (x^2 + 1) \bmod 8051$, then, from the initial values $a = 2, b = 2$, we have

- when $i = 1$, $a = 5$, $b = 26$, then $\gcd(|x - y|, 8051) = 1$
- when $i = 2$, $a = 26$, $b = 7474$, then $\gcd(|x - y|, 8051) = 1$
- when $i = 3$, $a = 677$, $b = 871$, then $\gcd(|x - y|, 8051) = 97$
- when $i = 4$, $a = 7474$, $b = 1481$, then $\gcd(|x - y|, 8051) = 1$

3 Pollard's $p - 1$ algorithm

Let $n = pq$, where p, q are large primes. If $q|(p - 1)$, where q is also a large prime, then p is a strong prime. Otherwise, p is strong, and n can be factored by Pollard's $p - 1$ algorithm. For example, $p - 1 = 2p_1p_2p_3 \cdot p_k$ only includes small prime factors, where $p_0 = 2$. If all p_i, $i = 1, 2, \cdots, k$, $p_i < B$, where B is an integer, we will know that

$$p_0p_1p_2p_3 \cdot p_k|B! \Rightarrow (p - 1)|B! \Rightarrow B! = (p - 1) \cdot \alpha$$

Algorithm: Pollard's ρ Algorithm: Given a composite $n = pq$:

1. set $a = 2$.
2. For $i = 1, 2, \cdots, B$ do:
    a) Compute $a \equiv a^i \bmod n$.

   $d = gcd(a-1, n)$;

   if $(1 < d < n)$

   * return $p = d$;

   else

   * return failure.

After running the algorithm, we know $a \equiv 2^{B!} \bmod n$. That is, $a = 2^{B!} + kn = 2^{B!} + kpq = 2^{B!} + k'p$, where $k' = kq$. Then,

$$a \equiv 2^{B!} \bmod p$$

Based on the Fermat's Little Theorem, we know

$$2^{p-1} \equiv 1 \bmod p \Rightarrow (2^{p-1})^{\alpha} \equiv 1^{\alpha} \bmod p \Rightarrow 2^{B!} \equiv 1 \bmod p \Rightarrow a \equiv 1 \bmod p$$

Then,

$$p|(a-1) \Rightarrow a - 1 = p \cdot k'' \Rightarrow \gcd(a-1, n) = p$$

Example. Suppose $n = 15770708441$. If we set $B = 180$, then from the above algorithm, we can find that $a = 1162221425$ and d is computed to be 135979. In fact, the complete factorization of n into primes is

$$15770708441 = 135979 \times 115979$$

In this example, the factorization is successful because $135979 - 1 = 135978$ has only "small" prime factors:

$$135978 = 2 \times 3 \times 131 \times 173$$

Therefore, by taking $B \geq 173$, it will be the case that $135978|B!$, as desired.

References

[1] G. J. Simmons and M. J. Norris, Preliminary Comments on the MIT Public-key Cryptosystem, Cryptologia (1977).

[2] J. M. Pollard, A Monte Carlo Method for Factorization, BIT Numerical Mathematics (1975).

[3] H. Riesel, Prime Numbers and Computer Methods for Factorization, Birkhauser, 1994.

[4] Abdullah Darwish, Imad Khaled Salah, and Saleh Oqeili, Mathematical At- tacks on RSA Cryptosystem, Journal of Computer Science (2006).