RSA Encryption

CS 5158/6058 Data Security and Privacy

Spring 2018

Instructor: Boyang Wang

Exponentiation in Group

- Group G, group order m,
  - A function f_e G—>G: exponentiation on element g with integer e
    - If G is additive, $f_e(g) = e*g$,
    - If G is multiplicative, $f_e(g) = g^e$
- If gcd(e,m)=1, then f_e is a permutation (bijection)

Exponentiation in Group

- A function f_e G—>G: $f_e(g) = e*g$ (additive group)
  - If gcd(e,m)=1, then f_e is a permutation (bijection)

- E.g., $Z_5 = \{0, 1, 2, 3, 4\}$ is an additive group,
  - if e = 2, gcd(e,m) = gcd(2,5) = 1
  - $f_e(0) = 2*0 = 0$; $f_e(1) = 2*1 = 2$; $f_e(2) = 2*2 = 4$;
  - $f_e(3) = 2*3 = 6 = 1$ mod Z_5;
  - $f_e(4) = 2*4 = 8 = 3$ mod Z_5
  - f_e :{0, 2, 4, 1, 3} a permutation of Z_5

Exponentiation in Group

- A function f_e G—>G: $f_e(g) = e*g$ (additive group)
  - If gcd(e,m)=1, then f_e is a permutation (bijection)

- E.g., Z_6 ={0, 1, 2, 3, 4, 5} is an additive group,
  - if e = 2, gcd(e,m) = gcd(2,6) = 2 != 1
  - $f_e(0) = 2*0 = 0$; $f_e(1) = 2*1 = 2$; $f_e(2) = 2*2 = 4$;
  - $f_e(3) = 2*3 = 6 = 0 \bmod Z_6$;
  - $f_e(4) = 2*4 = 8 = 2 \bmod Z_6$
  - $f_e(5) = 2*5 = 10 = 4 \bmod Z_6$
  - f_e :{0, 2, 4} is not a permutation of Z_6

Exponentiation in Group

- Practice: Z_7 ={0, 1, 2, 3, 4, 5, 6} is an additive group,
  - Group order m = ?? identity ??
  - If e = 2, is f_e a permutation of Z_7 ?
  - Compute $f_e(g)$, for all the elements in Z_7
  - $gcd(e, m) = gcd(2, 7) = 1$, f_e is a permutation
  - $f_e(0) = 2*0 = 0$; $f_e(1) = 2*1 = 2$; $f_e(2) = 2*2 = 4$;
  - $f_e(3) = 2*3 = 6$; $f_e(4) = 2*4 = 8 = 1 \bmod Z_7$
  - $f_e(5) = 2*5 = 10 = 3 \bmod Z_7$
  - $f_e(6) = 2*6 = 12 = 5 \bmod Z_7$
  - f_e: {0, 2, 4, 6, 1, 3, 5}

Exponentiation in Group

- A function f_e G—>G: $f_e(g)$, group order is m
  - if ed = 1 mod m, then f_d is inverse of f_e
    - $f_d(f_e(g)) = g$

  - If G is additive

$$f_d(f_e(g)) = f_d(eg) = deg = (ed \mod m)g = g$$

  - If G is multiplicative

$$f_d(f_e(g)) = f_d(g^e) = (g^e)^d = g^{ed \mod m} = g^1 = g$$

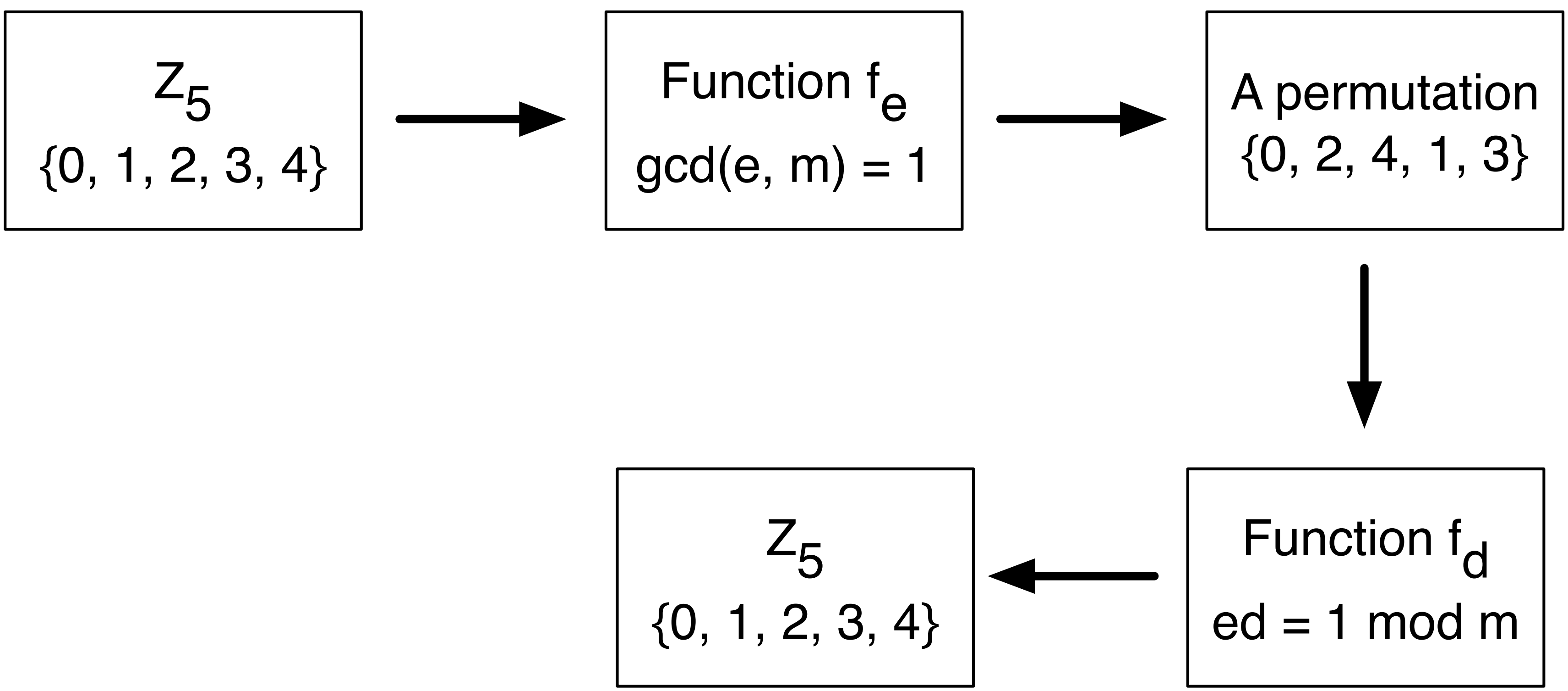
Exponentiation in Group

- Example: Z_5 =$\underline{\{0, 1, 2, 3, 4\}}$ is an additive group,
  - if e = 2, gcd(e,m) = gcd(2,5) = 1
  - f_e :$\underline{\{0, 2, 4, 1, 3\}}$ a permutation of Z_5

- If ed = 1 mod m, then f_d is inverse of f_e
  - e = 2, d = 3, ed = 3*2 mod m = 1 mod 5
  - $f_d(0)$ = 3*0 = 0; $f_d(2)$ = 3*2 = 1;
  - $f_d(4)$ = 3*4 = 12 = 2 mod Z_5; $f_d(1)$ = 3*1 = 3;
  - $f_d(3)$ = 3*3 = 9 = 4 mod Z_5
  - f_d:$\underline{\{0, 1, 2, 3, 4\}}$ inverse of f_e

Exponentiation in Group

- A function f_e G—>G: $f_e(g)$
  - If ed = 1 mod m, then f_d is inverse of f_e



Exponentiation in Group

- Practice: Z_7 ={0, 1, 2, 3, 4, 5, 6} is an additive group,
  - e = 2, f_e is a permutation, f_e: {0, 2, 4, 6, 1, 3, 5}
  - what is d =?? and compute f_d with all the inputs
  - e*d = 2*4 = 1 mod 7, d = 4
  - $f_d(0) = 4*0 = 0$; $f_d(2) = 4*2 = 1$;
  - $f_d(4) = 4*4 = 16 = 2$ mod Z_7;
  - $f_d(6) = 4*6 = 24 = 3$ mod Z_7; $f_d(1) = 4*1 = 4$
  - $f_e(3) = 4*3 = 12 = 5$ mod Z_7
  - $f_e(5) = 4*5 = 20 = 6$ mod Z_7
  - f_d: {0, 1, 2, 3, 4, 5, 6}, f_d is inverse of f_e

Group under Multiplication

- $Z_N = \{0, 1, 2, \ldots, N\text{-}1\}$ is a group under addition but not multiplication
  - If identity is 1, then some do not have inverse
  - E.g., 2 does not have an inverse, since 1/2 is not an element of Z_N, i.e. 2 is not invertible
- Find a group under multiplication mod N
  - Remove all the elements in Z_N that are not invertible
  - If b and N are relatively prime, i.e., gcd(b, N) = 1, then b is invertible mod N

Group under Multiplication

- Find a group under multiplication mod N
  - Remove elements in Z_N that are not invertible
  - If b and N are relatively prime, i.e., gcd(b, N) = 1, then b is invertible mod N

  - Z_N^* has all the integers in {1, 2, …, N-1} that are relatively prime to N

$$\mathbb{Z}_N^* = \{b \in \{1, ..., N-1\} \,|\, \gcd(b, N) = 1\}$$

  - Z_N^* is a multiplicative group

Group under Multiplication

- Example: N = 6, what are the elements in Z_6^* ?
  - $Z_6 = \{0, 1, 2, 3, 4, 5\}$,
    - remove 0 first
    - gcd(1, N) = 1, relatively prime
    - gcd(2, N) = 2, not relatively prime, remove 2
    - gcd(3, N) = 3, not relatively prime, remove 3
    - gcd(4, N) = 2, not relatively prime, remove 4
    - gcd(5, N) = 1, relatively prime
  - $Z_6^* = \{1, 5\}$ is a multiplicative group

Group under Multiplication

- Practice: N = 9, what are the elements in Z_9^* ?
  - Z_9= {0, 1, 2, 3, 4, 5, 6, 7, 8},
    - remove 0 first
    - gcd(1, N) = 1, gcd(2, N) = 1,
    - gcd(3, N) = 3 != 1, remove 3
    - gcd(4, N) = 1, gcd(5, N) = 1,
    - gcd(6, N) = 3 != 1, remove 6
    - gcd(7, N) = 1, gcd(8, N) = 1
  - Z_9^*= {1, 2, 4, 5, 7, 8}

Group under Multiplication

- Practice: $N = 11$, what are the elements in Z_{11}^* ?
  - $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
  - remove 0 first
  - $N=11$ is a prime, for any element $b>0$ in Z_{11}
    - $\gcd(b, N) = 1$
    - no need to remove any b

  - $Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Group under Multiplication

- Example: N = 9, what are the elements in Z_9^* ?
  - Z_9 ={0, 1, 2, 3, 4, 5, 6, 7, 8}; Z_9^*={1, 2, 4, 5, 7, 8}

- $|Z_N^*|$: Order of group Z_N^*
  - $|Z_N^*| = \phi(N)$, $\phi(\cdot)$ is called Euler phi function
  - The number of the integers in {1, 2, …, N-1} that are relatively prime to N
  - If N is a prime, then $\phi(N) = |Z_N^*| = N-1$
  - E.g.,N=7 is a prime, $|Z_7^*|=6$, Z_7^*={1, 2, 3, 4, 5, 6}

Group under Multiplication

- If N = pq, p, q are primes, $\phi(N)$ = $|Z_N^*|$ = (p-1)(q-1)
  - Why $|Z_N^*|$ is equal to (p-1)(q-1) ??

  - $|Z_N^*|$: the number of the integers in {1, 2, …, N-1} that are relatively prime to N
  - If a in {1, …, N-1} is not relatively prime to N
    - gcd(a, N) != 1
      - gcd(a, N) = p or gcd(a, N) = q
        - p | a or q | a

Group under Multiplication

- If $N = pq$, p, q are primes, then $|Z_N^*| = (p-1)(q-1)$
  - There are $(q-1)$ elements, s.t., $\gcd(a, N) = p$
    - Elements divided by p: $p, 2p, \ldots, (q-1)p$
  - There are $(p-1)$ elements, s.t., $\gcd(a, N) = q$
    - Elements divided by q: $q, 2q, \ldots, (p-1)q$

  - No. of elements s.t., $\gcd(a, N) \mathrel{!}= 1$
    - $(q-1) + (p-1)$
  - No. of elements s.t., $\gcd(a, N) = 1$
    - $N - 1 - (q-1) - (p-1) = (p-1)(q-1) = |Z_N^*|$

Group under Multiplication

- If N = pq, p, q are primes, then $|Z_N^*|$ = (p-1)(q-1)
- Example: N = 6 = 2*3, Z_6 = {0, 1, 2, 3, 4, 5}
    - p = 2, q = 3, p and q are primes
    - (q-1) = 2 elements, s.t., gcd(a, N) = p = 2
        - a = {2, 4}
    - (p-1) = 1 elements, s.t., gcd(a, N) = q = 3
        - a = {3}
    - Remove {0}, {2, 4} and {3}
    - Z_6^* = {1, 5} $|Z_6^*|$ = (2-1)*(3-1) = 2

- If N = pq, p, q are primes, then $|Z_N^*|$ = (p-1)(q-1)
- Practice: N = 21 = 3*7, Z_{21} = {0, 1, 2, …, 20, 21}
  - What are the elements in Z_{21}^* ?
  - How many elements in Z_{21}^*? Or $\phi(N)$= $|Z_{21}^*|$ = ?
  - p = 3, q = 7, p and q are primes
  - (q-1) = 6 elements, s.t., gcd(a, N) = p = 3
    - a = {3, 6, 9, 12, 15, 18}
  - (p-1) = 2 elements, s.t., gcd(a, N) = q = 7
    - a = {7, 14}
  - Remove {0}, {3,6,9,12,15,18} and {7,14}
  - Z_{21}^* = {1,2,4,7,8,11,13,14,16,17,19,20}
  - $|Z_{21}^*|$ = (3-1)*(7-1) = 2*6 =12

Group under Multiplication

- If group order is m, then $g^m = 1$, for any g in G
  - Exponentiation on element g with integer m is equal to group identity 1

- Z_N^* is a multiplicative group mod N
  - Exponentiation on element g with integer $|Z_N^*|$ is equal to group identity 1

$$g^{|\mathbb{Z}_N^*|} = g^{\phi(N)} = 1 \mod N$$

Group under Multiplication

- Z_7 = {0, 1, 2, 3, 4, 5, 6}, N=7, group order is m=7
- Z_7^*= {1, 2, 3, 4, 5, 6}, N=7, group order is m=6

$$g^{|\mathbb{Z}_N^*|} = g^{\phi(N)} = 1 \mod N$$

  - $1^6 = 1 \bmod N$, $2^6 = 64 = 1 \bmod N$,
  - $3^6 = 729 = 1 \bmod N$, $4^6 = 4096 = 1 \bmod N$,
  - $5^6 = 15625 = 1 \bmod N$, $6^6 = 46656 = 1 \bmod N$

- Z_7 is additive, Z_7^* is multiplicative

Group under Multiplication

- Z_6 = {0, 1, 2, 3, 4, 5}, N=2*3, group order is m=6
- Z_6*= {1, 5}, N=2*3, group order is m=(2-1)(3-1)=2

$$g^{|\mathbb{Z}_N^*|} = g^{\phi(N)} = 1 \mod N$$

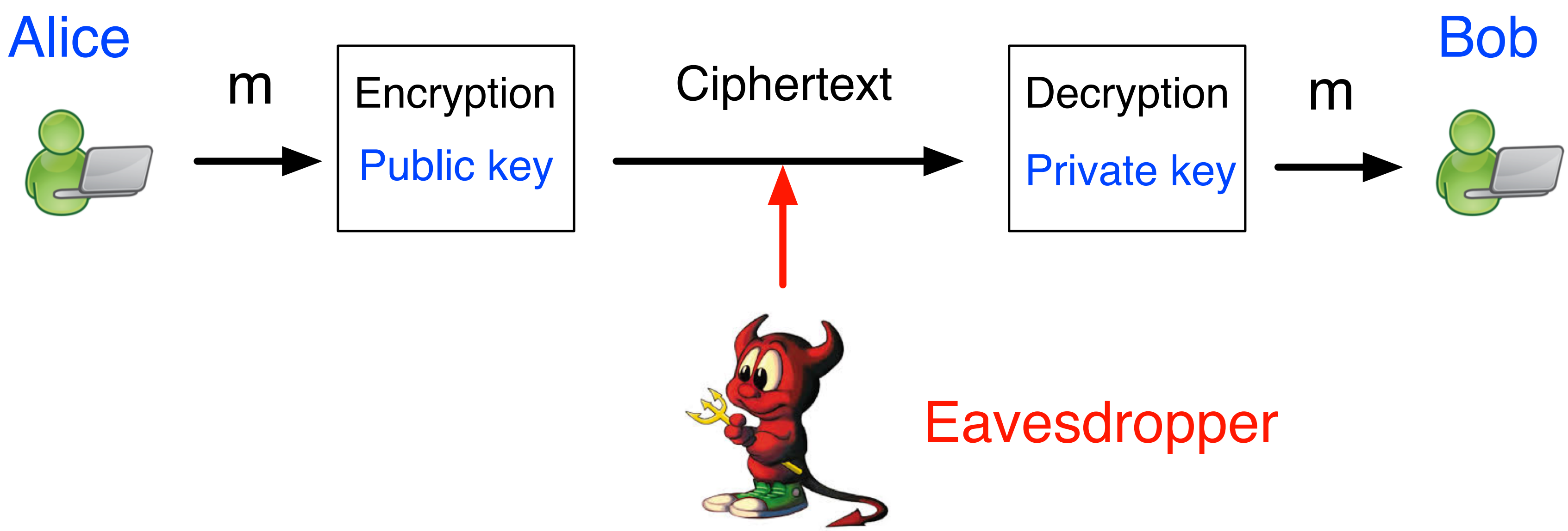
  - 1^2 = 1 mod N, 5^2 = 25 = 1 mod N,
- Z_6 is additive, Z_6* is multiplicative

Group under Multiplication

- Group G, order m
  - A function f_e G—>G: $f_e(g) = g^e$
  - If gcd(e, m)=1, then f_e is a permutation
  - ed =1 mod m, then f_d is inverse of f_e

- Group Z_N^*, order m = $|Z_N^*|$ = $\phi(N)$
  - A function f_e Z_N^*—>Z_N^*: $f_e(g) = g^e$
  - If gcd(e, $|Z_N^*|$)=1, then f_e is a permutation
  - ed =1 mod $|Z_N^*|$, then f_d is inverse of f_e

Public-Key Encryption



- Alice obtains Bob' public key from <u>public channels</u>
- Alice encrypts with public key
- Bob decrypts with private key

Public-Key Encryption

- PKE includes 3 algorithms

- KeyGen: given a security parameter 1^n, output a pair of keys (pk, sk), where pk is public and sk is private.
- Enc: given a public key pk and a message m, output a ciphertext c
- Dec: given a private key sk and a ciphertext c, output a message m.

One-Way Function

- One-way function is used in public-key crypto
  - Easy to compute
  - Hard to invert: (<u>with polynomial-time algorithm)</u>
  - E.g., factoring, discrete-log problem

- Factoring (integer factorization)
  - Assume p,q are <u>large primes</u>
  - Easy: p, q —> N = p*q
  - Hard: N —> p,q

RSA

- Rivest-Shamir-Adleman (RSA), 1978
  - Widely used today, SSL/TLS, email, HTTPS, etc.
  - ACM Turing award in 2002

Textbook RSA

- KeyGen: given a security parameter 1^n, generate two n-bit primes p, q, compute $N = pq$, choose e s.t. $\gcd(e, \phi(N)) = 1$, compute $d = e^{-1} \mod \phi(N)$, output public key $pk = (N, e)$, private key $sk = d$

- Enc: given a message m and a public key $pk = (N, e)$, return $c = m^e \mod N$

- Dec: given a ciphertext c and a private key $sk = d$, return $m = c^d \mod N$

Correctness

- For group $Z_N{}^*$ $g^{|\mathbb{Z}_N^*|} = g^{\phi(N)} = 1 \mod N$
- We know in RSA:

$$ed = 1 \mod \phi(N) \qquad \mathsf{Enc}_{pk}(m) = c = m^e \mod N$$

$$\begin{aligned} \mathsf{Dec}_{sk}(c) = c^d &= (m^e)^d \\ &= m^{ed \mod \phi(N)} \\ &= m \mod N \end{aligned}$$

- m, c are elements of group $Z_N{}^*$
- e, d are integers

Textbook RSA

- <u>Example:</u> $p*q = 17*23 = 391 = N$
    - $\phi(N) = |Z_N^*| = (p-1)(q-1) = 16*22 = 352$
    - choose e, s.t. $\gcd(e, \phi(N)) = 1$
    - $e = 3$, $\gcd(3, 352) = 1$
    - $d = 235$, $e*d = 3*235 = 705 = 1 \bmod 352$
    - $pk = (N, e) = (391, 3)$, $sk = d = 235$

    - Given $m=158$, $c=m^e \bmod N = 158^3 = 295 \bmod 391$
    - Given $c=295$, $m=c^d \bmod N = 295^{235} = 158 \bmod 391$

Textbook RSA

- Practice: p*q = 11*7 = 77 = N
    - $\phi(N)$ = $|Z_N^*|$ = (p-1)(q-1) = 10*6 = 60
    - choose e, s.t. gcd(e, $\phi(N)$) = 1

- Can we choose e = 3 in KeyGen?
    - No, gcd(e, $\phi(N)$) = gcd(3, 60) = 3 != 1

- Can we choose e = 7 in KeyGen?
    - Yes, gcd(e, $\phi(N)$) = gcd(7, 60) = 1

Textbook RSA

- <u>Practice</u>: p*q = 11*7 = 77 = N
  - $\phi(N)$ = $|Z_N^*|$ = (p-1)(q-1) = 10*6 = 60
  - choose e, s.t. gcd(e, $\phi(N)$) = 1
  - e = 7,
  - d = 43, ed = 7*43 = 1 mod 60
  - What is pk =? what is sk =?
    - pk = (N, e) = (77, 7), sk = d = 43
  - Given m = 2, what is c = m^e ?
    - c = m^e = 2^7 = 128 = 51 mod 77

Additional Reading

Chapter 8, *Introduction to Modern Cryptography, Drs. J. Katz and Y. Lindell, 2nd edition*