Public Key Cryptography

CS 363 Computer Security

Review questions

On average, ______ of all possible keys must be tried in order to achieve success with a brute-force attack.

A one-fourth

B half

C two-thirds

D three-fourths

Review questions

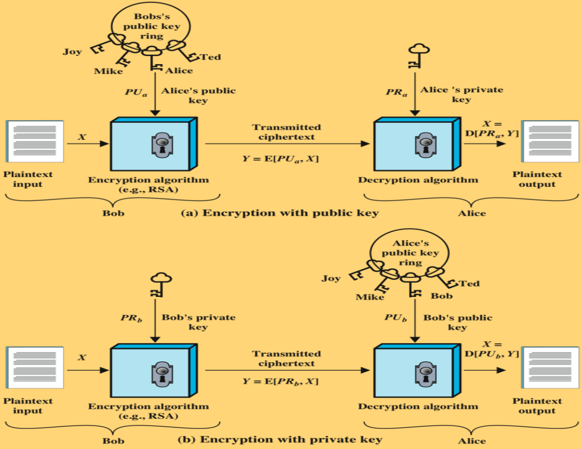
Consider a very simple symmetric block encryption algorithm, in which 64 bits blocks of plaintext are encrypted are encrypted using a 128-bit key. Encryption is defined as

$$C = (P \oplus K_0) + K_1 \pmod{2^{64}}$$

where C is plaintext; K is secret key; K_0 is the leftmost 64 bits of K; K_1 is the rightmost 64 bits of K.

- Show the decryption equation.
- Suppose an adversary has access to two sets of plaintexts and their corresponding ciphertexts and wish to determine K. Can you do it?

Public Key Encryption



(a) Encryption with public key

(b) Encryption with private key

Public-Key Cryptography

Requirements for Public-Key Cryptosystems (1976)

- useful if either key can be used for each role
- computationally easy to create key pairs
- computationally easy for sender knowing public key to encrypt messages
- computationally easy for receiver knowing private key to decrypt ciphertext
- computationally infeasible for opponent to otherwise recover original message
- computationally infeasible for opponent to determine private key from public key

Computation Complexity

- P = Problems we can solve efficiently: Sorting a large set of numbers
- NP = Problems we can check the solution efficiently
  - 41659 is a factor of 1735472281
  - 3-coloring of a graph
  - Lots of NP problems do not yet have efficient solutions
- Efficiency is with respect to typical computer (Turing machine) not crazy computers (Quantum, Random)

P ?= NP

- Ask Dr. Barry Witman?

P ?= NP

- Ask Dr. Barry Witman?
- an extremely hard problem

P ?= NP

- Ask Dr. Barry Witman?
- an extremely hard problem
  - The Clay Mathematics Institute in Boston is currently offering $ 1 million if you can solve it

P ?= NP

- Ask Dr. Barry Witman?
- an extremely hard problem
    - The Clay Mathematics Institute in Boston is currently offering $ 1 million if you can solve it
    - Try it? then maybe retire? Not enough?

P ?= NP

- Ask Dr. Barry Witman?
- an extremely hard problem
    - The Clay Mathematics Institute in Boston is currently offering $ 1 million if you can solve it
    - Try it? then maybe retire? Not enough?
- Implication to Public-Key Cryptosystem
    - Many NP problems can be turned into a public-key cipher

P ?= NP

- Ask Dr. Barry Witman?
- an extremely hard problem
  - The Clay Mathematics Institute in Boston is currently offering $ 1 million if you can solve it
  - Try it? then maybe retire? Not enough?
- Implication to Public-Key Cryptosystem
  - Many NP problems can be turned into a public-key cipher
  - Easy to compute (validate the answer) but difficult to do the inverse (find the solution) unless you have the private key

P ?= NP

- Ask Dr. Barry Witman?
- an extremely hard problem
  - The Clay Mathematics Institute in Boston is currently offering $ 1 million if you can solve it
  - Try it? then maybe retire? Not enough?
- Implication to Public-Key Cryptosystem
  - Many NP problems can be turned into a public-key cipher
  - Easy to compute (validate the answer) but difficult to do the inverse (find the solution) unless you have the private key
  - also known as One-Way Trapdoor Function

P ?= NP

- Ask Dr. Barry Witman?
- an extremely hard problem
  - The Clay Mathematics Institute in Boston is currently offering $ 1 million if you can solve it
  - Try it? then maybe retire? Not enough?
- Implication to Public-Key Cryptosystem
  - Many NP problems can be turned into a public-key cipher
  - Easy to compute (validate the answer) but difficult to do the inverse (find the solution) unless you have the private key
  - also known as One-Way Trapdoor Function

A few facts about module arithmetic

- If $a \equiv b \pmod{N}$, then $a = k \cdot N + b$ for some integer k
- Multiplicative inverse: $ab \equiv 1 \pmod{N}$
  - Condition: a and b are relatively prime to N, i.e. they share no common factors other than 1.
  - Why?

Modular Exponentiation Example (Prime Modulus)

x	0	1	2	3	4	5	6	7	8	9	10	11
$0^x \mod 11$	?	0	0	0	0	0	0	0	0	0	0	0
$1^x \mod 11$	1	1	1	1	1	1	1	1	1	1	1	1
$2^x \mod 11$	1	2	4	8	5	10	9	7	3	6	1	2
$3^x \mod 11$	1	3	9	5	4	1	3	9	5	4	1	3
$4^x \mod 11$	1	4	5	9	3	1	4	5	9	3	1	4
$5^x \mod 11$	1	5	3	4	9	1	5	3	4	9	1	5
$6^x \mod 11$	1	6	3	7	9	10	5	8	4	2	1	6
$7^x \mod 11$	1	7	5	2	3	10	4	6	9	8	1	7
$8^x \mod 11$	1	8	9	6	4	10	3	2	5	7	1	8
$9^x \mod 11$	1	9	4	3	5	1	9	4	3	5	1	9
$10^x \mod 11$	1	10	1	10	1	10	1	10	1	10	1	10
$11^x \mod 11$	1	0	0	0	0	0	0	0	0	0	0	0

Another Modular Exponentiation Example (Composite Modulus)

x	0	1	2	3	4	5	6
$0^x \mod 6$	?	0	0	0	0	0	0
$1^x \mod 6$	1	1	1	1	1	1	1
$2^x \mod 6$	1	2	4	2	4	2	4
$3^x \mod 6$	1	3	3	3	3	3	3
$4^x \mod 6$	1	4	4	4	4	4	4
$5^x \mod 6$	1	5	1	5	1	5	1
$6^x \mod 6$	1	0	0	0	0	0	0

Square-and-Multiply Algorithm

To compute an exponent like 25^{19}, we could multiply 25 by itself 18 times, but this is *extremely* inefficient. It is better to express the exponent in base 2 $\left(19 = 2^4 + 2^1 + 2^0\right)$ and square successively.

Computing

$$\begin{aligned} 25^2 &= 625 \\ 25^4 &= 625^2 = 390,625 \\ 25^8 &= 390,625^2 = 152,587,890,625 \\ 25^{16} &= 152,587,890,625^2 = 23,283,064,365,386,962,890,625 \end{aligned}$$

and

$$\begin{aligned} 25^{19} &= 25^{16} \cdot 25^2 \cdot 25^1 = (23,283,064,365,386,962,890,625)(625)(25) \\ &= 363,797,880,709,171,295,166,015,625 \end{aligned}$$

only requires 6 multiplications instead of 18.

Modular Square-and-Multiply Algorithm

Compute $25^{19} \mod 103$.

$$\begin{aligned} 25^2 &= 625 \equiv 7 \mod 103 \\ 25^4 &= 7^2 \equiv 49 \mod 103 \\ 25^8 &= 49^2 = 2401 \equiv 32 \mod 103 \\ 25^{16} &= 32^2 = 1024 \equiv 97 \mod 103 \end{aligned}$$

and

$$\begin{aligned} 25^{19} &\equiv 25^{16} \cdot 25^2 \cdot 25^1 \mod 103 \\ &\equiv (97)(7)(25) \mod 103 \\ &\equiv 16,975 \mod 103 \\ &\equiv 83 \mod 103. \end{aligned}$$

The *Mathematica* command `PowerMod` implements something like the square-and-multiply algorithm.

Computing Modular Exponents on a Computer

Contemporary public key algorithms use big numbers like these.

$$2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$$

$$\begin{aligned}2^{256} = 115,792,089,237,316,195,423,570,985,008,687,907,\\ 853,269,984,665,640,564,039,457,584,007,913,129,639,936\end{aligned}$$

$$\begin{aligned}2^{512} = 13,407,807,929,942,597,099,574,024,998,205,846,127,479,365,\\ 820,592,393,377,723,561,443,721,764,030,073,546,976,801,874,\\ 298,166,903,427,690,031,858,186,486,050,853,753,882,811,946,\\ 569,946,433,649,006,084,096\end{aligned}$$

$$\begin{aligned}2^{1024} = 179,769,313,486,231,590,772,930,519,078,902,473,361,797,697,\\ 894,230,657,273,430,081,157,732,675,805,500,963,132,708,477,\\ 322,407,536,021,120,113,879,871,393,357,658,789,768,814,416,\\ 622,492,847,430,639,474,124,377,767,893,424,865,485,276,302,\\ 219,601,246,094,119,453,082,952,085,005,768,838,150,682,342,\\ 462,881,473,913,110,540,827,237,163,350,510,684,586,298,239,\\ 947,245,938,479,716,304,835,356,329,624,224,137,216\end{aligned}$$

Euler's ϕ Function

Definition Let $n \in \mathbb{N}$. Then the Euler phi function $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n.

Euler's ϕ Function

Definition Let $n \in \mathbb{N}$. Then the Euler phi function $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n.

Example: $\phi(26) = 12$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26$$

Euler's ϕ Function

Definition Let $n \in \mathbb{N}$. Then the Euler phi function $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n.

Example: $\phi(26) = 12$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26$$

Example: $\phi(11) = 10$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$$

Euler's ϕ Function

Definition Let $n \in \mathbb{N}$. Then the Euler phi function $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n.

Example: $\phi(26) = 12$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26$$

Example: $\phi(11) = 10$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$$

Example: $\phi(21) = 12$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21$$

More Examples - Euler's ϕ Function

Example: $\phi(16) = 8$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$$

More Examples - Euler's ϕ Function

Example: $\phi(16) = 8$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$$

Example: $\phi(27) = 18$

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27$

Rules

Can we deduce rules for

- $\phi(p)$,
- $\phi(pq)$, and
- $\phi\left(p^k\right)$,

where p and q are primes and k is a positive integer?

Summary of Facts about Euler's ϕ Function

- If p is a prime number, then $\phi(p) = p - 1$.
- If p and q are distinct primes, then $\phi(pq) = \phi(p)\phi(q)$.
- If p is prime and k is a positive integer, then $\phi\left(p^k\right) = p^k - p^{k-1}$.

Lemma for Euler's Theorem

Lemma: Let a and n be positive integers such that $n > 1$ and $\gcd(a, n) = 1$. If $S = \{a_1, a_2, \ldots, a_{\phi(n)}\}$ is the set of distinct positive integers less than n and relatively prime to n, then $T = \{aa_1, aa_2, \ldots, aa_{\phi(n)}\}$ is a permutation of S.

Proof: First note that if a and a_k, $k = 1, 2, \ldots, \phi(n)$, are both relatively prime to n, then aa_k is also relatively prime to n. Now we only have to show that the elements of T are distinct. If $aa_j = aa_k$ for some j and k, then multiplying by a^{-1} gives that $a_j = a_k$.

Multiples of Sets of Relatively Prime Numbers

The numbers in the set $\{1, 3, 7, 9\}$ are the $\phi(10) = 4$ positive integers less than 10 that are relatively prime to 10.

If $a \in \{1, 3, 7, 9\}$, then the numbers $\{a \cdot 1, a \cdot 3, a \cdot 7, a \cdot 9\}$ are a permutation of $\{1, 3, 7, 9\}$.

If so, then

$$\begin{aligned} 1 \cdot 3 \cdot 7 \cdot 9 &\equiv (a \cdot 1)(a \cdot 3)(a \cdot 7)(a \cdot 9) \mod 10 \\ &= a^4 (1 \cdot 3 \cdot 7 \cdot 9) \mod 10 \\ &= a^{\phi(10)} (1 \cdot 3 \cdot 7 \cdot 9) \mod 10. \end{aligned}$$

Since $\gcd(1 \cdot 3 \cdot 7 \cdot 9, 10) = 1$, $a^{\phi(10)} \equiv 1 \mod 10$.

Euler's Theorem

Theorem: If a and n are positive integers such that $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.

Proof: If $n = 1$, then the result is obvious. Suppose $n > 1$ and let $S = \left\{a_1, a_2, \ldots, a_{\phi(n)}\right\}$ be the set of positive integers less than n that are relatively prime to n. In addition, let $T = \left\{aa_1, aa_2, \ldots, aa_{\phi(n)}\right\}$. By the lemma, each element of S is congruent to a distinct element of T. Multiplying the elements of S and T implies that

$$\begin{aligned} a^{\phi(n)} a_1 a_2 \ldots a_{\phi(n)} &= (aa_1)(aa_2) \ldots \left(aa_{\phi(n)}\right) \\ &\equiv a_1 a_2 \ldots a_{\phi(n)} \mod n. \end{aligned}$$

Since the elements of S are relatively prime to n, the product $a_1 a_2 \ldots a_{\phi(n)}$ is relatively prime to n, so $\left(a_1 a_2 \ldots a_{\phi(n)}\right)^{-1}$ exists and $a^{\phi(n)} \equiv 1 \mod n$.

Two Corollaries of Euler's Theorem

Fermat's Little Theorem: If p is a prime number that does not divide the integer a, then $a^{p-1} \equiv 1 \mod p$.

Euler's Corollary: Let a be an integer that is relatively prime to both of the distinct primes p and q. Then $a^{(p-1)(q-1)} \equiv 1 \mod pq$.

Diffie-Hellman Key Exchange

- Alice and Bob agree *publicly* on a large prime number p and an integer $q < p$. For the sake of illustration, let $p = 23$ and $q = 5$.
- Alice and Bob then each *privately* choose a number less than p. For example, Alice chooses $a = 9$ and Bob chooses $b = 20$.
- Alice computes

  $$A = q^a \mod p = 5^9 \mod 23 \equiv 11 \mod 23$$

  and sends it to Bob. Bob computes

  $$B = q^b \mod p = 5^{20} \mod 23 \equiv 12 \mod 23$$

  and sends it to Alice.
- Alice computes

  $$K = B^a \mod p = 12^9 \mod 23 \equiv 4 \mod 23.$$

  Bob also computes K, but in a different way:

  $$K = A^b \mod p = 11^{20} \mod 23 \equiv 4 \mod 23.$$

If Eve intercepts A, B, p, and q, then she can, in principle, solve for a and b by solving

$$A = q^a \mod p \qquad B = q^b \mod p.$$

This is called the *discrete log problem* and it is very hard to solve for large p.

Another Diffie-Hellman Example

- Let $p = 156696463087$ and $q = 94477582661$.
- Alice chooses $a = 63102091160$ and Bob chooses $b = 23629131076$.
- Alice computes

$$A = q^a \mod p = 94477582661^{63102091160} \mod 156696463087 = 908653225$$

and Bob computes

$$B = q^b \mod p = 94477582661^{23629131076} \mod 156696463087 = 1340136561.$$

- Alice sends A to Bob and Bob sends B to Alice and they both compute

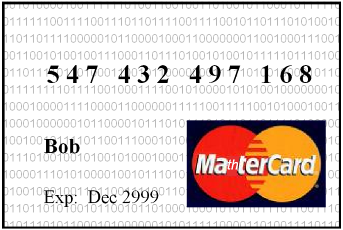
$$K = A^b \mod p = 908653225^{23629131076} \mod 156696463087 = 67301429533$$
$$K = B^a \mod p = 1340136561^{63102091160} \mod 156696463087 = 67301429533.$$

The common key K can be used as the key for another encryption system like a Vigenère cipher. The digits in K can be partitioned into pairs, reduced modulo 26, and converted to letters.

$$067301429533 \to 062101161707 \to \text{GVBQRH}$$

Note that, unlike RSA, the Diffie-Hellman system does not transmit a secret message. Sender and receiver secretly compute the same number that neither knows in advance.

Classroom Exercise



- Alice and Bob use the Diffie-Hellman key exchange to establish a common key. ($p = 239$ and $q = 123$)[1]
- They agree to use a Vigenère cipher mod 10.
- Bob encrypts and transmits his Mathtercard number to Alice.
- Alice decrypts Bob's Mathtercard number to the amazement of one and all.

[1] https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html

The RSA Cryptosystem

RSA is a concatenation of the first initials of the last names of Ron Rivest, Adi Shamir, and Leonard Adleman, who together invented the RSA algorithm at MIT in 1978.

For Alice, the Key Center selects two large prime numbers p and q and easily computes $\phi(pq) = (p-1)(q-1)$. The Key Center then selects any integer e relatively prime to $\phi(pq)$ and computes its multiplicative inverse $\mod \phi(pq)$. Finally, the key center issues Alice the public keys e and pq and the private key $e^{-1} \mod \phi(pq)$.

RSA

- Two keys e and $d = e^{-1}$ used for Encryption and Decryption
- The keys are interchangeable:
  $M = D(d, E(e, M)) = D(e, E(d, M))$

The security of this method relies on the difficulty of factoring the product pq.

- Best known algorithm is exponential
- Largest number ever factored   800-bit (232 digits)
- RSA uses key lengths ranges from 1024 bits to 4096 bits

The RSA Cryptosystem (continued)

If Bob wants to send Alice a integer message m, he uses her public keys to compute

$$c = m^e \mod pq,$$

which he sends to her in the clear. When Alice receives c, she computes

$$\begin{aligned} c^{e^{-1}} \mod pq &\equiv (m^e)^{e^{-1}} \mod pq \\ &\equiv m^{ee^{-1}} \mod pq \\ &\equiv m^{1+k\phi(pq)} \mod pq \quad \text{for some integer } k \\ &\equiv m \cdot \left(m^{\phi(pq)}\right)^k \mod pq \\ &\equiv m(1)^k \mod pq \quad \text{by Euler's Theorem} \\ &\equiv m. \end{aligned}$$

If Eve intercepts the message, she can only read it if she can solve $m^e \equiv c \mod pq$ for m. That is, Eve has to find the e^{th} root of c modulo pq.

Sending an Example Message with RSA

Alice publishes her public keys $e = 7$ and $pq = 77$ for all to see. To send the message $m = 25 < pq$ to Alice, Bob computes

$$c = m^e \mod pq = 25^7 \mod 77 \equiv 53 \mod 77$$

and sends it to Alice. Alice uses her private key, $e^{-1} = 43$ to compute

$$\begin{aligned} c^{e^{-1}} \bmod pq &= 53^{43} \mod 77 \\ &\equiv 25 \mod 77 \\ &= m. \end{aligned}$$

If Eve intercepts $c = 53$, she can decipher it if she can compute

$$m^7 \mod 77 = 53.$$

Another Example RSA Exchange

The Key Center chooses the primes

$$p = 80467184927 \quad \text{and} \quad q = 55547251337$$

for Alice and computes $\phi(pq) = 4469730945384912561136$. The Key Center then chooses e, computes $e^{-1} \mod pq$, and sends Alice her public keys:

$$e = 4073619424605228097289$$
$$pq = 4469730945520926997399$$

and her private key

$$e^{-1} \mod \phi(pq) = 2559385183601091556777.$$

Bob sends message $m = 12345678901234567890$ to Alice by computing the cipher

$$\begin{aligned} c &= m^e \mod pq \\ &= 12345678901234567890^{4073619424605228097289} \mod 4469730945520926997399 \\ &\equiv 3469293885116137999704 \mod 4469730945520926997399. \end{aligned}$$

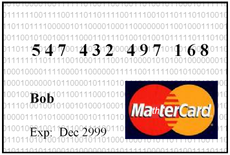
Alice decrypts the cipher c by computing

$$\begin{aligned} c^{e^{-1}} \mod pq &= 3469293885116137999704^{2559385183601091556777} \\ &= 12345678901234567890 \mod 4469730945520926997399. \end{aligned}$$

What is m?

The message m could be

- a private number like a credit card number.



- the key for a symmetric cipher system if Alice and Bob want to exchange a lot of data.
- a concatenation of ASCII codes for a brief text message. For example, the ASCII equivalent of "Test on Friday" is

$$84\ 101\ 115\ 116\ 32\ 111\ 110\ 32\ 70\ 114\ 105\ 100\ 97\ 121\ 46,$$

  so maybe

$$m = 084101115116032111110032070114105100097121046.$$

Security of RSA

Brute force attack

- trying all possible private keys
- defense is to use a large key space, however this slows speed of execution

- RSA-140 (decimal digits):Factored in 1 month using 200 machines in 1999
- RSA-155: Factored in 3.7 months using 300 machines in 1999
- RSA-160: Factored in 20 days in 2003
- RSA-200: Factored in 18 month in 2005
- RSA-210, RSA-220, RSA-232, . . . , RSA-2048

More attacks on RSA

Mathematical attacks: in effort to factoring the product of two primes

Timing attacks:

- depend on the running time of the decryption algorithm
- comes from a completely unexpected direction and is a ciphertext-only attack
- countermeasures: constant exponentiation time, random delay, blinding

Chosen ciphertext attacks: attack exploits properties of the RSA algorithm

Digital Signatures

If Bob sends a message to Alice, how does Alice know that Bob really sent it?

Bob can encipher his “signature” with his own private key and when Alice receives his message, she can decrypt it using Bob’s public key.

Digital Signatures - An Example

Bob sends a surprising message to Alice:

> *Alice, I've decided to major in cs. It's the coolest! Bob (125010690)*

Bob knows that Alice won't believe that he actually sent the message, so he digitally signed it by enciphering his name (in ASCII) using his own private key. Alice finds that Bob's public keys are $e = 1234567891$ and $pq = 176391331$, and she computes

$$\begin{aligned} 125010690^e \mod pq &= 125010690^{1234567891} \mod 176391331 \\ &\equiv 66111098 \mod 176391331 \end{aligned}$$

Since the decrypted digital signature matches his name (in ASCII),

$$66\ 111\ 098 \rightarrow \text{B o b}$$

Alice is sure that Bob actually sent the message. Congratulations Bob!

Reminder & Next ...

- Bradley Vasilik's presentation: Bitcoin, 1:40 pm in Tuesday class of Feb 6th
- James's presentation: Bitcoin, 1:40 pm in Tuesday class of Feb 8th
- Project 1 due by 11:59pm on Feb 11th
- Hash functions