Week 7: Asymmetric encryption

Dr. Qublai K. Ali Mirza

University of Gloucestershire

qalimirza@glos.ac.uk

Overview

Assignment requirements

- Individual-based
- Critical evaluation of the Orion case study from a *cybersecurity consultant*
- Use your understanding of cryptography concepts and approaches to protect *both*:
  - Data at rest
  - Data in transit
- You are more than welcome to use *any* reputable external resources and academic articles
- Submission deadline: 25th May 2018

UNIVERSITY OF GLOUCESTERSHIRE

Prime & Co-Prime

- Prime
  - A composite number, a number that can be divided by other numbers. E.g. 12.
  - A prime number is a number greater than 1 that is only divisible by 1 and itself.
- Co-Prime
  - A co-prime or relatively prime numbers are two numbers that have no common divisors other than 1.
  - 4 and 15 are co-prime.
  - Factors of 4 are 1 and 2.
  - Factors of 15 are 1, 3 and 5.

UNIVERSITY OF GLOUCESTERSHIRE

Euler's Totient

- Given an integer of n, how many numbers are co-prime to n?
- That number is called the Euler's totient.
- The Euler phi function, or simply totient.
- Symbol for the totient of a number is ϕ.

Example

- Find the ϕ of $n = 8$
- First, list *all* numbers up to $n - 1$
- So in this case, it would be: $1, 2, 3, 4, 5, 6, 7$
- Then identify all co-prime numbers to n. So this would be: $1, 3, 5, 7$
- So the answer then is $(\phi)(8) = 4$

UNIVERSITY OF GLOUCESTERSHIRE

Asymmetric encryption

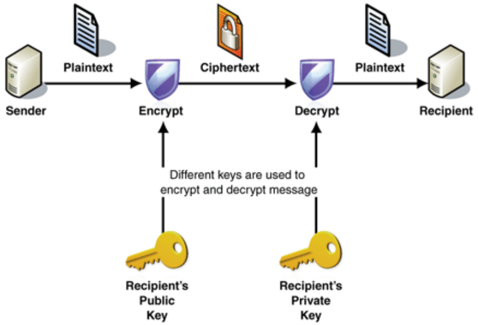

Figure: Asymmetric encryption overview, from [4]

Overview

- The purpose of the algorithm is to allow two users to securely exchange a key that can used for the ongoing symmetric encryption of messages.
- The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms.
- The algorithm is only used for the exchange of secret keys.

How it works

- Two users Alice and Bob wish to communicate.
- They agree two primes $q = 353$ (Alice) and $a = 3$ (Bob).
- Such that $a < q$ and a is a primitive root of q.
- They both select random secret (private) keys. Do not share these keys.
- Alice chooses X_A such that $X_A < q = 97$.
- Bob chooses X_B such that $X_B < q = 233$.

- They now compute a common secret key.
- Alice computes:

$$K_{AB} = y_B^{X_A} mod\ q = 160.$$

- Bob computes:

$$K_{AB} = y_A^{X_B} mod\ q = 160.$$

- An attacker knows the following information:
$q = 353; a = 3; Y_A = 40; Y_B = 248$

Overview

- Was one of the first public key schemes
- Developed in 1977 by three MIT mathematicians Ron Rivest, Adi Shamir and Len Adleman
- Based on modular arithmetic and prime numbers
- supports various key lengths of 1024, 2048, and 4096-bits
- Published in 1978

Public Key Encryption

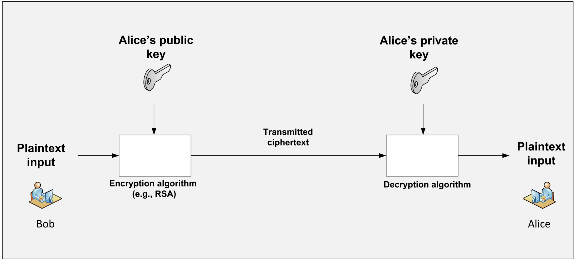

Figure: Encryption with a public key

Encryption/Decryption

- Encryption

$$c = ENCRYPT(m) = m^e mod\ n$$

- Decryption

$$m = DECRYPT(c) = c^d mod\ n$$

RSA Algorithm

1. Choose prime numbers p and q
2. Compute $n = p \times q$
3. Select d and e, such that
    1. d is co-prime to $(p-1) \times (q-1)$, and
    2. $(e \times d) mod\ ((p-1) * (q-1)) = 1$
4. Discard p and q
5. Public key is the pair (e,n) and private key is the pair (d,n)
6. Operation (plaintext p, ciphertext c)
    - Encrypt: $c = p^e mod\ n$
    - Decrypt: $p = c^d mod\ n$

RSA Example

1. Select two prime numbers $p = 17$ and $q = 11$
2. Calculate $n = pq = 17 \times 11 = 187$
3. Calculate $\phi(n) = (p - 1)\ (q - 1)\ = 16 \times 10 = 160$
4. Select e such that e is relatively prime to $\phi(n) = 160$ and less than $\phi(n)$; we choose e=7.
5. Public key $KU = [7, 187]$.
6. Determine d such that $de\ mod\ 160 = 1$ and $d < 160$.
7. The value is for $d = 23$, because $23 \times 7 = 161 = 10 \times 160 + 1$
8. Private Key $KR = [23, 187]$

UNIVERSITY OF GLOUCESTERSHIRE

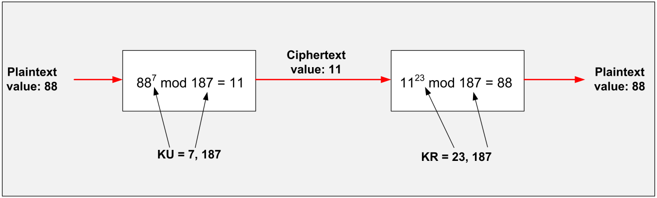

Figure: RSA operation, based on example

Overview

- While both RSA and Diffie-Hellman allows for the use of different keys for encryption/decryption, they require very large numbers (at least 200 bits)
- This puts significant limitations on key storage/processing especially on devices with limited processing power
- In order to get around this limitation, we can use *Elliptic Curve Cryptography (ECC)*

Elliptic Curve

- Constructed using the following equation where x, y, a, and b are real numbers:

$$y^2 = x^3 + ax + b$$

- Consists of the following characteristics:
  - There is a point at inifinity ∞ denoted by 0
  - Symmetric about the X-axis
  - Given two points P and Q, their addition $P + Q = R$ is a reflection of the intersection

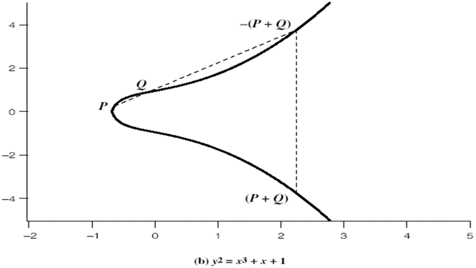

Figure: Real elliptic curve, obtained from [3]

Finite Elliptic Curves

- Variation of the usual elliptic curve, but key difference: the coefficients are all *integers*
- Uses integers modulo prime p for both variables and coefficients
- The equation for the finite elliptic curve then becomes:

$$y^2 mod\ \ p = (x^2 + ax + b)\ \ mod\ \ p$$

Finite Elliptic Curves

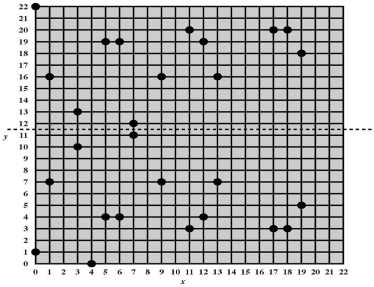

Figure: Elliptic curve confined to mod 23, from [2]

Elliptic Curve Cryptography

- In order to use ECC as a cryptography tool, there are six “domain parameters” that we need to take into account:
  - p: The prime number which all point operations will be take *modulo* with
  - a, b: The coefficients of the elliptic curve
  - G: The base point of the curve
  - n: The number of integer points on the curve
  - h: The *cofactor* of the curve

Key Generation

- Generating a public/private key pair is quite similar to the traditional public key encryption approaches
- This involves first obtaining as a private key a random integer d_A such that:

$$0 < d_A < n$$

- Once obtained, the private key d_A can then be used to obtain public key P_A such that:

$$P_A = d_A \cdot G$$

UNIVERSITY OF GLOUCESTERSHIRE

Encryption

- Suppose Alice wants to send a message to Bob using ECC
- First Alice selects as a private key a random integer d_A
- She then calculates the corresponding public key P_A which is then sent to Bob
- She also calulates $S = d_A \cdot P_B$ from which the symmetric key is derived for encryption

UNIVERSITY OF GLOUCESTERSHIRE

Decryption

- When Bob receives the encrypted message along with R, he obtains the symmetric key S by using the following equation:

$$S = d_B \cdot R$$

- Once obtained, S is then used to derive the symmetric key by multiplying it with Alice's public key P_A

UNIVERSITY OF GLOUCESTERSHIRE

Strengths and Limitations

- Strengths
  - Smaller key sizes
  - Requires less computation power
  - Suitable for embedded systems
- Limitations
  - Relatively slower than RSA
  - Requires a truly random RNG
  - Can be susceptible against attacks

Bringing it all together

- Today we looked at *Asymmetric encryption*
- We looked at how public key encryption works
- We also looked at RSA encryption as well
- Next week: *The application of cryptography*

Post-sessional work

- Using the article by [1] (available on *Moodle*) as a starting point, write a critical review on how asymmetric encryption is used to protect sensitive data
- Upload your completed work to *Moodle* before next *Monday*.

References I

- P Fanfara, E Danková, and M Dufala. "Usage of asymmetric encryption algorithms to enhance the security of sensitive data in secure communication". In: *Applied Machine Intelligence and Informatics (SAMI), 2012 IEEE 10th International Symposium on*. IEEE. 2012, pp. 213–217.
- *Section 10.3. Elliptic Curve Arithmetic.* https://flylib.com/books/en/3.190.1.92/1/. Accessed: 2018-03-28.
- William Stallings. *Cryptography and network security: principles and practices*. Pearson Education India, 2006.

UNIVERSITY OF GLOUCESTERSHIRE

References II

X.509 Technical Supplement. https://msdn.microsoft.com/en-us/library/aa480610.aspx. Accessed: 2018-01-17. 2005.

Q & A