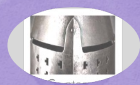


Chapter 10

Other Public-Key Cryptosystems

1

Other PKCS

- In this module we will be looking in detail at other public key cryptosystems other than RSA
- We will look at
  - Diffie-Hellman Key exchange
  - Elliptic Curve Cryptography (ECC)
- For ECC we will look primarily at the basis of thee algebraic structure that the algorithm is built on i.e. elliptic curve arithmetic (ECA)
- For ECA we will look at how
  - the operations work
  - we can create groups
  - we can create a one-way trapdoor function

2

Diffie-Hellman Key Exchange

- First published public-key algorithm
- A number of commercial products employ this key exchange technique
- Purpose is to enable two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages
- The algorithm itself is limited to the exchange of secret values
- Its effectiveness depends on the difficulty of computing discrete logarithms

3

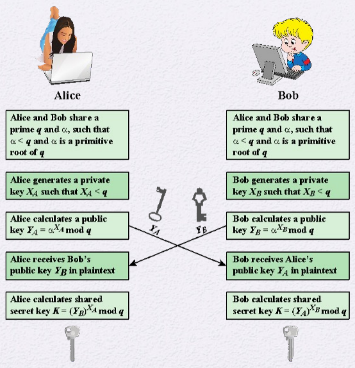


Figure 10.1 Diffie-Hellman Key Exchange

4

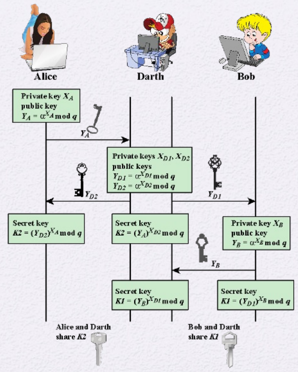


Figure 10.2 Man-in-the-Middle Attack

5

Elliptic Curve Arithmetic

- Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA
  - The key length for secure RSA use has increased over recent years and this has put a heavier processing load on applications using RSA
- Elliptic curve cryptography (ECC) is showing up in standardization efforts including the IEEE P1363 Standard for Public-Key Cryptography
- Principal attraction of ECC is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead

6

Elliptic Curves

- Elliptic curves are not ellipses. They are so named because they are described by **cubic equations,** similar to those used for calculating the circumference of an ellipse
- They are defined by the equation
  $y^2 = x^3 + ax + b$ or $y = \sqrt{x^3 + ax + b}$

7

Elliptic Curves

- For given values of *a* and *b*, the plot consists of positive and negative values of *y* for each value of *x*. Thus, each curve is symmetric about $y = 0$
- Also included in the definition of an elliptic curve is a single element denoted *O* and called the *point at infinity* or the **zero point**
- In geometry, a point at infinity or ideal point is an idealized limiting point at the "end" of each line

8

Elliptic Curves

- The set of points E(*a,b*) consists of all of the points (*x,y*) that satisfy the equation of the curve together with the element *O*.
- The shape of each curve is determined by the pair (*a,b*).
- So, an elliptic curve can be denoted as E(*a,b*), where **a** and **b** are the values used in the equation that defines the curve

9

Abelian Group

- A set of elements with a binary operation, denoted by •, that associates to each ordered pair (a, b) of elements in G an element $(a \cdot b)$ in G, such that the following axioms are obeyed:

(A1) Closure: If a and b belong to G, then $a \bullet b$ is also in G

(A2) Associative: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all a, b, c in G

(A3) Identity element: There is an element e in G such that $a \bullet e = e \bullet a = a$ for all a in G

(A4) Inverse element: For each a in G there is an element a' in G such that $a \bullet a' = a' \bullet a = e$

(A5) Commutative: $a \bullet b = b \bullet a$ for all a, b in G

10

Abelian Group

- For an elliptic curve to form an abelian group, its values of a and b must fulfill the inequality
  - $4a^3 + 27b^2 \neq 0$

11

Elliptic Curve Arithmetic

- The fundamental operation in elliptic curve arithmetic is addition (of two points on the curve)
  - This is very different from addition in regular arithmetic
- Multiplication is defined as multiple addition
- Identity element is the *point at infinity* or the ***zero point***

12

Elliptic Curve Arithmetic

- If three points on an elliptic curve lie on a straight line, their sum is taken as O
  - P + Q + R = O
  - P + Q = -R (for two points with different x coordinates)
- For a point P = (x,y) we have that -P =(x,-y)
- P + (-P) = O (for two points with the same x coordinates)

13

Elliptic Curve Arithmetic

- To add a point to itself
  - Q + Q = 2Q = -S
  - Where S is the point of intersection of the line tangent to Q and the curve
- You can only multiply a point with an integer value. You cannot multiply two points
  - 3P = P + P + P

14

Addition in ECA

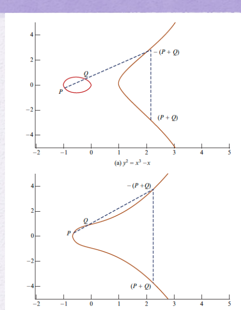


Figure 10.4 Example of Elliptic Curves

15

Finite Fields

- Creating elliptic curves that are defined over finite fields require additional steps
  - These will not be covered here. You are however encouraged to look this up
- There are two kinds of elliptic curves defined over finite fields
  - **Prime Curves** – with variables and coefficients taking values between *(0 – p-1)* and all calculations are done mod p
  - **Binary Curves** - with variables and coefficients taking values in GF(2^m) and calculations performed over GF(2^m)

16

Elliptic Curve Cryptography (ECC)

- Addition operation in ECC is the counterpart of modular multiplication in RSA
- Multiple addition is the counterpart of modular exponentiation

To form a cryptographic system using elliptic curves, we need to find a "hard problem" corresponding to factoring the product of two primes or taking the discrete logarithm

- *Q=kP*, where *Q, P* belong to a prime curve
- Is "easy" to compute *Q* given *k* and *P*
- But "hard" to find *k* given *Q*, and *P*
- Known as the elliptic curve logarithm problem

17

Security of Elliptic Curve Cryptography

- Depends on the difficulty of the elliptic curve logarithm problem
- Fastest known technique is "Pollard rho method"
- Compared to factoring, can use much smaller key sizes than with RSA
- For equivalent key lengths computations are roughly equivalent
- Hence, for similar security ECC offers significant computational advantages

18

Table 10.3

Comparable Key Sizes in Terms of Computational Effort for Cryptanalysis (NIST SP-800-57)

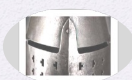
Symmetric key algorithms	Diffie-Hellman, Digital Signature Algorithm	RSA (size of n in bits)	ECC (modulus size in bits)
80	$L = 1024$ $N = 160$	1024	160–223
112	$L = 2048$ $N = 224$	2048	224–255
128	$L = 3072$ $N = 256$	3072	256–383
192	$L = 7680$ $N = 384$	7680	384–511
256	$L = 15{,}360$ $N = 512$	15,360	512+

Note: L = size of public key, N = size of private key

19

Summary

- Define Diffie-Hellman Key Exchange
- Understand the Man-in-the-middle attack



- Understand Elliptic curve arithmetic
- Present an overview of elliptic curve cryptography

20