Introduction to Cryptology

Tutorial-07
DH Key-Exchange/Sharing System

09.05.2023, v43

Design Summary for
A Basic Diffie-Hellmann (DH) Public Key Exchange System

In case that you have a prime:

1. If you have a prime number **p** and you know how to factor $\varphi(p) = p1\ p2\ ..pt$, then use the prime p to generate GF(p).
2. Find a primitive element α by checking that $\alpha^{p1} \neq 1$ and $\alpha^{p2} \neq 1$, $\alpha^{p1p2} \neq 1$ ….. and $\alpha^{pt} \neq 1$. α is selected randomly.
3. Publish GF(p) and α in a public directory. The system is ready for use. The strength of your system is equal to the smallest prime factor of $\varphi(p)$.

In case that you do not have a prime:

1. Select a strong prime number p such that p-1 = 2 q where q is a prime.
   A possible procedure is to use Pocklington's Theorem to find such a prime:
   - Select **N = 2q + 1** where q is a large prime. Check if the resulting N is prime using Pocklington's Theorem
   - If N is prime, take p=N and generate GF(p)
2. Find a primitive element $\boldsymbol{\alpha}$ in GF(p) by selecting any non-zero random value and checking if its order is p-1. The order of any element in GF(p) is a divisor of p-1=2q. That is the order can be either **1, 2, q or 2q**. If $\alpha^2 \neq 1$ and $\alpha^q \neq 1$ then the order of α is 2q and α is a primitive element. Repeat 2 until you get a primitive element.
3. Publish GF(p) and α in a public directory. The system is ready for use.

The procedure is simillar over the extension field GF(2^m) !

Problem 7-1:

1. Find a primitive element $\boldsymbol{\alpha}$ to set up a DH public-key exchange system using the prime number 43.
2. Generate DH common key Z_{ab} for two users A and B having $X_a = 3$ and $X_b = 7$ as secret keys respectively.

Solution 7-1:

1. To find a primitive element $\boldsymbol{\alpha}$ in GF(43) we select randomly $\boldsymbol{\alpha} = 3$ and check if it is a primitive element.
   3 is primitive if its order is a divisor of $\varphi(p) = 43 - 1 = 42 = 2 . 3 . 7$
   The order of any element is one of these divisors: 1, 2, 3, 7, 6, 14, 21 or 42

   Computing the order of 3: $3^2 = 9 \neq 1$, $3^3 = 27 \neq 1$, $3^6 = 41 = -2 \neq 1$, $3^7 = -6 \neq 1$, $3^{14} = 36 \neq 1$, $3^{21} = -1 \neq 1$ => 3 is a primitive element.

2.

DH Public directory:
GF (43)
$\boldsymbol{\alpha} = 3$
$Y_a = 3^{Xa} = 3^3 = 27$
$Y_b = 3^{Xb} = 3^7 = -6 = 37$

Common key is $Z_{ab} = (Y_b)^{Xa} = (Y_a)^{Xb}$
$= (3^7)^3 = 3^{21} = -1 = 42$

Problem 7-2:

1. Generating one strong prime with the prime 23 (N = 2 * 23 + 1)
2. Find a primitive element $\boldsymbol{\alpha}$ to set up a DH public-key exchange system using the generated strong prime number from exercise 1.
3. Generate DH common key Z_{ab} for two users A and B having $X_a = 24$ and $X_b = 2$ as secret keys respectively.
4. What is the probability that a randomly selected element is a primitive element?

Solution 7-2:

1. Let us try to check if N= 2 * 23 + 1 = 47 is prime. Using Pocklington's Theorem:
   If the following conditions hold then 47 is a prime:
   1. $\gcd(2^{(47-1)/23} - 1, 47) = \gcd(2^2 - 1, 47) = \gcd(3,47) = 1$ => is true
   2. $2^{47-1} = 1$ mod 47 or in Z_{47} => is true
   3. $F = 23 > \sqrt{47}$ => 23 > 6 => is true

   As all conditions hold, 47 is for sure a prime
2. To find a primitive element $\boldsymbol{\alpha}$ in GF(47) we select randomly $\boldsymbol{\alpha} = 2$ and check if it is a primitive element. 2 is primitive if its order is a divisor of $\varphi(p) = 47 - 1 = \mathbf{46} = 2 * 23$.
   The order of any element is one of the divisors: 1, 2, 23 or 46
   Computing the order of 2: $2^2 = 4 \neq 1$, $2^{23} = 48 = 1$ => 2 is not a primitive element ! Check another element!

Solution 7-2 Cont.:

Computing the order of 5: Possible orders are 1, 2, 23 or 46
$5^1 = 5 \neq 1$, $5^2 = 25 \neq 1$, $5^{23} = 46 = -1 \neq 1$ (all modulo 47)
Therefore, the order of 5 must be 46 and 5 is a primitive element.
which may be used in the DH public directory

DH Public Directory:
GF (47)
$\boldsymbol{\alpha} = 5$
$Y_a = 5^{24} = -5 = 42$
$Y_b = 5^2 = 25$

In General
The modulus in the exponent is Euler function $\varphi(m)$

$\varphi(p) = 47 - 1 = \mathbf{46}$

3. Common key is $Z_{ab} = (Y_b)^{Xa} = (Y_a)^{Xb}$
   $= (5^{24})^2 = 5^{48 \bmod 46} = 5^{48-46} = 5^2 = \mathbf{25}$

4. The number of primitive elements is $\varphi(46) = \varphi(2x23) = (2-1)(23-1) = \mathbf{22}$
   Prob. of having a Primitive element = 22/46 = **47.8%**

Problem 7-3:

1. Select a irreducible polynomial and a primitive element $\boldsymbol{\alpha}$ to set up a DH public-key exchange system over **GF(2^{10})**.
2. Generate DH common key Z_{ab} for two users A and B having $X_a = 12$ and $X_b = 4$ as secret keys respectively.
3. What is the probability that a randomly selected element is a primitive element?

Solution 7-3:

1. Let us select the irreducible polynomial for GF(2^{10}) as $p(x) = x^{10} + x^3 + 1$
   This polynomial is also primitive as its period is $1023 = 2^{10} - 1$ (see table of irreducible polynomials). The order of x is $2^{10} - 1$.
   A possible primitive element is $\boldsymbol{\alpha} = x$ = **0000000010** as its order is $2^{10} - 1 = 1023 = 3 * 11 * 31$.
   Possible elements orders in GF(2^{10}) are the divisors of 1023 = 1, 3, 11, 31, 33, 93, 341, 1023.
   A randomly selected element $\boldsymbol{\alpha}$ is primitive if: $\boldsymbol{\alpha}^3 \neq 1$ and $\boldsymbol{\alpha}^{11} \neq 1$ and , $\boldsymbol{\alpha}^{31} \neq 1$ and $\boldsymbol{\alpha}^{33} \neq 1$ and $\boldsymbol{\alpha}^{93} \neq 1$, $\boldsymbol{\alpha}^{341} \neq 1$.
   Many other primitive elements can be selected as $\boldsymbol{\alpha}^i$ for which **gcd(1023,i)=1,** for example:
   $x^{10} = x^3 + 1$ = 0000001001 is a primitive element
   $x^{20} = (x^3 + 1)^2 = x^6 + 1$ = 0001000001 is also a primitive element

Solution 7-3 Cont.:

DH Public directory:
GF (2^{10}), p(x) = $x^{10}+x^3+1$
$\alpha = x = 0000000010$

$Y_a = x^{12} = x^5 + x^2$
$Y_b = x^4$

2. Public keys are $Y_a = x^{12} = x^{10}\, x^2 = (x^3+1)x^2 = x^5 + x^2$
   $Y_b = x^4$

   Common key is $\mathbf{Z_{ab}} = (Y_b)^{Xa} = (Y_a)^{Xb}$
   $= (x^5 + x^2)^4$
   $= x^{20} + x^8 = x^6 + 1 + x^8$
   Z_{ab} = 0101000001

3. The number of primitive elements is $\varphi(1023) = \varphi(3 * 11 * 31) = (3-1)(11-1)(31-1) =$ **600**
   Prob. of having a Primitive element = 600/1023 **= 58.6%**

7

Problem 7-4:

A Diffie-Hellman (DH) public key exchange system uses GF(2^6) deploying the irreducible polynomial $p(x) = x^6 + x^3 + 1$.

1. For $\beta = x$, compute β^i for i = 1 to 10. What is the multiplicative order of x?
2. Which multiplicative orders are possible for elements in GF(2^6)?
3. Prove that the element $\delta = 1+x = 000011$ is a primitive element.
4. Compute the multiplicative order of δ^{14}
5. Use the element δ as a public element in the above GF(2^6) and compute the DH public keys Y_a and Y_b and the shared secret key Z_{ab} for users A and B having the secret keys X_a=42 and X_b=14.
   Compute the binary vectors for Y_a and Y_b and Z_{ab} by making use of the following: $\delta^7 = x^5 + x^2$, $\delta^{21} = 1 + x^3$,
6. What is the probability of getting an element with order 21 if the element is picked up randomly from GF(2^6)?.
7. For any element α from GF(2^6), compute t for which $\alpha^{-1} = \alpha^t$.
   Compute then x^{-1} mod p(x) using that result. (Hint make use of the results in 1)
   Verify your result.

8

Solution 7-4:

1. $P(x) = x^6 + x^3 + 1 = 0 \quad => \quad x^6 = x^3 + 1$
   $x^1 = x$
   $x^2 = x^2$
   $x^3 = x^3$
   $x^4 = x^4$
   $x^5 = x^5$
   $x^6 = x^3 + 1$
   $x^7 = x^4 + x$
   $x^8 = x^5 + x^2$
   $x^9 = x^6 + x^3 = x^3 + x^3 + 1 = 1$
   $x^{10} = x \qquad => \quad ord(x) = 9$
2. Possible orders are the divisors of $2^6 - 1 = 63$
   Divisors of 63 are: 1,3,7,9,21 and 63
3. $(x+1)^1 = x+1 \neq 1$
   $(x+1)^3 = (x+1)^2 . (x+1) = (x^2+1) . (x+1) = x^3+x^2+x+1 \neq 1$
   $(x+1)^7 = ((x+1)^3)^2 . (x+1) = (x^3+x^2+x+1)^2 . (x+1) = (x^6+x^4+x^2+1) . (x+1)$
   $= x^7+x^5+x^3+x+x^6+x^4+x^2+1 = x^4+x+x^5+x^3+x+x^3+1+x^4+x^2+1 = x^5+ x^2 \neq 1$
   $(x+1)^9 = (x+1)^7 . (x+1)^2 = (x^5+x^2) . (x^2+1) = x^7+x^4+x^5+x^2 = x^4+x+x^4+x^5+x^2 = x^5+x^2+x \neq 1$
   $(x+1)^{21} = ((x+1)^7)^3 = (x^5+x^2)^3 = (x^5+x^2)^2 . (x^5+x^2) = (x^{10}+x^4) . (x^5+x^2) = (x+x^4) . (x^5+x^2)$
   $= x^6+x^3+x^9+ x^6 = x^6+x^3+x^6 + x^3+ x^6 = x^3+1 \neq 1 \quad => ord(x+1) = 63$

9

Solution 7-4 Cont.:

4. $ord(\delta^{14}) = \dfrac{ord(\delta)}{\gcd(ord(\delta), i)} = \dfrac{63}{\gcd(63,14)} = \dfrac{63}{7} = 9$

5. User A:
   $X_a = 42$,
   $Y_a = (x+1)^{42} \bmod (x^6+x^3+1)$
   $= ((x+1)^{21})^2 = (x^3+1)^2$
   $= x^6+1 = x^3+1 + 1 = x^3$
   $= 001000$

   Public directory GF(2^6)
   $\delta = x+1$, $P(x) = x^6 + x^3 + 1$
   $Y_a = x^3 \quad = 001000$
   $Y_b = x^4+x = 010010$

   User B:
   $X_b = 14$,
   $Y_b = (x+1)^{14} = ((x+1)^7)^2 = (x^5+x^2)^2$
   $= x^{10}+x^4 = x^4 + x$
   $= 010010$

   Common secret key for users A and B
   $Z_{ab} = (x+1)^{42\,.\,14 \bmod 63} = (x+1)^{21} = x^3+1$
   $Z_{ab} = x^3 + 1 = 001001$

6. # of all non-zero elements: $2^6 - 1 = 63$
   # of elements with order 21: $\varphi(21) = \varphi(7 . 3) = 6 . 2 = 12$
   Pr(element's order=21) = (12 / 63) . 100 = 19.05 %

10

Solution 7-4 Cont.:

7. For any element t, $\alpha^{-1 \text{ mode } 63} = \alpha^{-1+63} = \alpha^{62} = \alpha^t \rightarrow t = 62$
   $x^{-1} = x^{62} = (x^9)^6\, x^8 = (1)^6\, x^8 = x^8$
   $x^{-1} = x^8 = x^5 + x^2$
   Verification:
   $x . x^{-1} = x . x^8 = x^9 = 1$ (see 1)

11

Homework:

A Diffie-Hellman public-key exchange system is setup over GF(2^4) using the primitive polynomial $P(x) = x^4 + x + 1$.

1. Compute all exponents of x up to 15 and state the corresponding binary patterns
2. Which one of the following elements is primitive? 0011, 1111. Select it as the primitive element for DH public directory
3. What is the probability that a randomly selected element is primitive?
4. Compute DH common key for two users A and B having Xa=**11** and Xb=**7** as secret keys respectively.

(Final exam 2004)

12