[SKIP TO CONTENT](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/#content)

* [HOME](http://bithin.wordpress.com/)
* [ABOUT](http://bithin.wordpress.com/about/)

[](http://bithin.wordpress.com/)

[← Facts behind HTTPS](http://bithin.wordpress.com/2012/02/21/facts-behind-https/)

[Socket programming using PHP →](http://bithin.wordpress.com/2012/02/26/socket-programming-using-php/)

FEBRUARY 22, 2012 · 9:28 AM

[↓ Jump to Comments](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/#comments)

[**Simple explanation for Elliptic Curve Cryptographic algorithm ( ECC )**](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/)

[Elliptic Curve Cryptography](http://www.certicom.com/index.php/ecc) (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing [public-key cryptography](https://www.rsa.com/rsalabs/node.asp?id=2165).

[](http://bithin.files.wordpress.com/2012/02/ecc.jpg)

I  assume that those who are going through this article will have a basic understanding of [cryptography](https://en.wikipedia.org/wiki/Cryptography) ( terms like encryption and decryption ) .

The equation of an elliptic curve is given as,

[http://bithin.files.wordpress.com/2012/02/eccequation.png?w=500](http://bithin.files.wordpress.com/2012/02/eccequation.png)

Few terms that will be used,

**E -> Elliptic Curve**

**P -> Point on the curve**

**n -> Maximum limit ( This should be a prime number )**

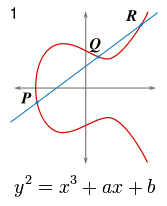
[](http://bithin.files.wordpress.com/2012/02/ell-curve.png)

Fig 3

The fig 3 show are simple elliptic curve.

**Key Generation**

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver’s public key and the receiver will decrypt its private key.

Now, we have to select a number**‘d’**within the range of**‘n’**.

Using the following equation we can generate the public key

**Q = d \* P**

**d** = The random number that we have selected within the range of (**1 to n-1** ). **P**is the point on the curve.

**‘Q’ is the public key**and**‘d’ is the private key.**

**Encryption**

Let ‘m’ be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details. All the advance research on ECC is done by a company called [certicom](http://www.certicom.com/index.php/ecc).

Conside*‘m’* has the point*‘M’* on the curve*‘E’.*Randomly select ‘k’ from [1 - (n-1)].

Two cipher texts will be generated let it be **C1**and**C2**.

**C1 = k\*P**

**C2 = M + k\*Q**

C1 and C2 will be send.

**Decryption**

We have to get back the message ‘m’ that was send to us,

**M = C2 – d \* C1**

M is the original message that we have send.

**Proof**

How does we get back the message,

M = C2 – d \* C1

‘M’ can be represented as ‘C2 – d \* C1′

C2 – d \* C1 = (M + k \* Q) – d \* ( k \* P )          ( C2 = M + k \* Q and C1 = k \* P )

=  M + k  \* d \* P – d \* k \*P          ( canceling out k \* d \* P )

= M  ( Original Message )

[About these ads](http://en.wordpress.com/about-these-ads/)

**Share this:**

* [Email](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/?share=email)
* [Facebook](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/?share=facebook)
* [Twitter](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/?share=twitter)
* [LinkedIn](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/?share=linkedin)

Loading...

[3 Comments](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/#comments)

Filed under [Security](http://bithin.wordpress.com/category/security-2/)

Tagged as [advance research](http://bithin.wordpress.com/tag/advance-research/), [cryptography](http://bithin.wordpress.com/tag/cryptography/),[cryptography algorithm](http://bithin.wordpress.com/tag/cryptography-algorithm/), [ecc](http://bithin.wordpress.com/tag/ecc/), [elliptic curve cryptography](http://bithin.wordpress.com/tag/elliptic-curve-cryptography/), [encryption and decryption](http://bithin.wordpress.com/tag/encryption-and-decryption/)

**3 Responses to *Simple explanation for Elliptic Curve Cryptographic algorithm ( ECC )***

1. http://0.gravatar.com/avatar/6dfba8921391e33361aef77eee275027?s=48&d=identicon&r=G*eeeweq*

[October 21, 2013 at 9:40 am](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/#comment-173)

how private key known to receiver?

[Reply](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/?replytocom=173#respond)

* + http://0.gravatar.com/avatar/38828150a8c70f5fdc8a17291b7837c4?s=48&d=identicon&r=G[*bithin*](http://bithin.wordpress.com/)

[December 17, 2013 at 12:07 am](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/#comment-174)

It will be nice if you can spend some time in reading this<http://en.wikipedia.org/wiki/Public-key_cryptography>. I am sure you will be able to understand.

[Reply](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/?replytocom=174#respond)

1. http://0.gravatar.com/avatar/ff55bdc6aafd3cff7b8fc464ceefc9c1?s=48&d=identicon&r=G*aleena joy*

[January 2, 2014 at 5:56 pm](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/#comment-227)

Could you please say about Elliptical curve diffie-hellman key exchange

[Reply](http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/?replytocom=227#respond)

**Leave a Reply**

Top of Form



Bottom of Form

* **Archives**
  + [December 2013](http://bithin.wordpress.com/2013/12/) (1)
  + [February 2013](http://bithin.wordpress.com/2013/02/) (1)
  + [December 2012](http://bithin.wordpress.com/2012/12/) (1)
  + [April 2012](http://bithin.wordpress.com/2012/04/) (1)
  + [February 2012](http://bithin.wordpress.com/2012/02/) (3)
  + [September 2011](http://bithin.wordpress.com/2011/09/) (2)
  + [July 2011](http://bithin.wordpress.com/2011/07/) (2)
  + [June 2011](http://bithin.wordpress.com/2011/06/) (5)
  + [May 2011](http://bithin.wordpress.com/2011/05/) (6)
  + [March 2011](http://bithin.wordpress.com/2011/03/) (1)
  + [February 2011](http://bithin.wordpress.com/2011/02/) (1)
  + [January 2011](http://bithin.wordpress.com/2011/01/) (1)
* **Calender**

| February 2012 | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **M** | **T** | **W** | **T** | **F** | **S** | **S** |
| [« Sep](http://bithin.wordpress.com/2011/09/) | | |  | [Apr »](http://bithin.wordpress.com/2012/04/) | | |
|  | | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | [21](http://bithin.wordpress.com/2012/02/21/) | [22](http://bithin.wordpress.com/2012/02/22/) | 23 | 24 | 25 | [26](http://bithin.wordpress.com/2012/02/26/) |
| 27 | 28 | 29 |  | | | |

* **Categories**
  + [College](http://bithin.wordpress.com/category/college-2/)
  + [Drupal](http://bithin.wordpress.com/category/drupal/)
  + [General](http://bithin.wordpress.com/category/general/)
  + [InCTF](http://bithin.wordpress.com/category/inctf/)
  + [My life](http://bithin.wordpress.com/category/my-life/)
  + [Operating Systems](http://bithin.wordpress.com/category/operating-systems/)
  + [Security](http://bithin.wordpress.com/category/security-2/)
  + [Uncategorized](http://bithin.wordpress.com/category/uncategorized/)
  + [web](http://bithin.wordpress.com/category/web/)
* [**My Delicious**](http://del.icio.us/bithin2007)
  + [Leaflet-dvf](http://humangeo.github.io/leaflet-dvf/)
  + [yohanboniface/django-leaflet-storage · GitHub](https://github.com/yohanboniface/django-leaflet-storage)
  + [Serving Tiles](http://switch2osm.org/serving-tiles/)
  + [Multivariable Calculus](http://ocw.mit.edu/courses/mathematics/18-02-multivariable-calculus-fall-2007/assignments/)
  + [Individual grants](http://www.srtt.org/individual_grants/education_grants.htm)
* **Tags**

[advance research](http://bithin.wordpress.com/tag/advance-research/)[awareness](http://bithin.wordpress.com/tag/awareness/) [bittorrent](http://bithin.wordpress.com/tag/bittorrent/)[cleaning](http://bithin.wordpress.com/tag/cleaning/) [core store](http://bithin.wordpress.com/tag/core-store/) [cryptographic algorithm](http://bithin.wordpress.com/tag/cryptographic-algorithm/) [cryptography](http://bithin.wordpress.com/tag/cryptography/)[cryptography algorithm](http://bithin.wordpress.com/tag/cryptography-algorithm/) [ctf](http://bithin.wordpress.com/tag/ctf/) [digital signatures](http://bithin.wordpress.com/tag/digital-signatures/)[distributed system](http://bithin.wordpress.com/tag/distributed-system/) [drupal](http://bithin.wordpress.com/tag/drupal-2/)[Dynamic Memory Allocation](http://bithin.wordpress.com/tag/dynamic-memory-allocation/) [ecc](http://bithin.wordpress.com/tag/ecc/)[elliptic curve cryptography](http://bithin.wordpress.com/tag/elliptic-curve-cryptography/) [encryption and decryption](http://bithin.wordpress.com/tag/encryption-and-decryption/) [environment](http://bithin.wordpress.com/tag/environment/) [gmail](http://bithin.wordpress.com/tag/gmail/)[inctf](http://bithin.wordpress.com/tag/inctf-2/) [key agreement](http://bithin.wordpress.com/tag/key-agreement/) [memory allocation](http://bithin.wordpress.com/tag/memory-allocation/) [Operating Systems](http://bithin.wordpress.com/tag/operating-systems/) [peer-to-peer](http://bithin.wordpress.com/tag/peer-to-peer/) [research](http://bithin.wordpress.com/tag/research/) [secure socket layer](http://bithin.wordpress.com/tag/secure-socket-layer/) [security](http://bithin.wordpress.com/tag/security/) [socket programming](http://bithin.wordpress.com/tag/socket-programming/) [software-development](http://bithin.wordpress.com/tag/software-development/)[summer school](http://bithin.wordpress.com/tag/summer-school/) [technology](http://bithin.wordpress.com/tag/technology/) [torrent](http://bithin.wordpress.com/tag/torrent/)[Virtual Memory](http://bithin.wordpress.com/tag/virtual-memory/) [web application development](http://bithin.wordpress.com/tag/web-application-development/) [yahoo](http://bithin.wordpress.com/tag/yahoo/)

* **cluster map**

[[](http://www4.clustrmaps.com/user/d41dae53)](http://www4.clustrmaps.com/user/d41dae53)

* **Blog Stats**
  + 17,720 hits

· Bithin's Blog

[Blog at WordPress.com](http://wordpress.com/?ref=footer). · [The Pilcrow Theme](http://theme.wordpress.com/themes/pilcrow/).

[Follow](javascript:void(0))

**Follow “”**

Top of Form

Get every new post delivered to your Inbox.

Join 174 other followers



Bottom of Form

[Powered by WordPress.com](http://wordpress.com/signup/?ref=lof)