

- Home
- Reference
 - Number Theory
 - Cryptography
- Links
- Calendar
- Photos
- Blog
 - Vietnam
 - Technical
 - Number theory
 - Cryptography
- Online LaTeX
- Online Python
- Lunar Calendar

Highlight: Windows Server 2003 SDK

Comments Popular Latest Statistic

- Doctoral Degree vs. PhD: What's the Difference?**
Quite clear! [More...](#)
Date: 08/10/2010 - 10:32
- Tài liệu hướng dẫn thực hành**
def cesar_d(c,k): abc='ABCDEFGHIJKLMNOPQRSTUVWXYZ'; p=""; for i in range(len(c)): p += abc[(abc.index... [More...](#)
Date: 07/10/2010 - 09:38
- Tài liệu hướng dẫn thực hành**
def cesar(p,k): abc='ABCDEFGHIJKLMNOPQRSTUVWXYZ'; c=""; for j in range(len(p)): c += abc[(abc.index... [More...](#)
Date: 07/10/2010 - 06:32



Quick Search

Search...

This Day in History



The Mughal empire was a Muslim imperial power that ruled most of the Asian subcontinent between the 16th and 19th centuries. Led by Babur, the dynasty's founder, Mughal forces made an inroad into India in 1526, occupying Delhi in the first Battle of Panipat. Babur was succeeded by his son, who soon lost the empire to the Afghan Sher Khan. In 1556, Babur's grandson came to power and fought the army of Hemu in the Second Battle of Panipat. What cost Hemu the battle and, ultimately, his life? [More...](#) [Discuss](#)

Search on EntireWeb

Poll

What is your current operating system?

- Ubuntu
- Mac
- Window
- Other

Vote Results

Weather

Ho Chi Minh City, Ho Chi Minh City
27°C Cloudy
 Humidity: 72%
 Wind: NW at 11 mph

Idioms

- Every man has his faults (Nhân vô thập toàn)
- A friend in need is a friend indeed. (Gian nan mới hiểu bạn bè)

Who's online

We have 6 guests online

Location

- 203.162.44.37
- 106.667 : 10.75
- www.math.hcmuns.edu.vn
- Linux
- Chrome 7.0.5

Most Popular Tags

- C communication configure
- crypt cryptography device
- driver elliptic curve exercise
- guide kernel letter linux
- ma hoa microsoft module
- number theory port posix
- practice programming
- purpose serial sop
- statement

Site Ranking

Tài liệu hướng dẫn thực hành (DES)

Blog - Cryptography
 Written by **Thong D. Nguyen**
 Friday, 05 November 2010 14:49

User Rating: / 1
 Poor Best

Giới thiệu:

Mã DES là một mã lặp 16 vòng mã hóa một văn bản p dài 64 bit với một khóa dài 56 bit. Ở mỗi vòng, trạng thái wi được chia làm hai phần dài 32 bit là Li và Ri. Khóa Ki ở mỗi lần lặp dài 48 bit là một khóa được sinh ra từ khóa K ban đầu. Việc mã hóa được tiến hành như sau:

$$w_0 = (L_0, R_0) = IP(x)$$

$$w_i = (L_i, R_i) = g(L_{i-1}, R_{i-1}, K_i) = (R_{i-1}, L_{i-1} \oplus f(R_{i-1}, K_i))$$

$$c = IP^{-1}(R_{16}, L_{16})$$

Việc giải mã được thực hiện tương tự với hàm g⁻¹ cho bởi công thức:

$$(L_{i-1}, R_{i-1}) = g^{-1}(L_i, R_i, K_i) = (R_i \oplus f(L_i, K_i), L_i)$$

Hướng dẫn:

1. Hoán vị IP và nghịch đảo của nó được cho bởi bảng sau:

58	50	42	34	26	18	10	2	40	8	48	16	56	24	64	32
60	52	44	36	28	20	12	4	39	7	47	15	55	23	63	31
62	54	46	38	30	22	14	6	38	6	46	14	54	22	62	30
64	56	48	40	32	24	16	8	37	5	45	13	53	21	61	29
57	49	41	33	25	17	9	1	36	4	44	12	52	20	60	28
59	51	43	35	27	19	11	3	35	3	43	11	51	19	59	27
61	53	45	37	29	21	13	5	34	2	42	10	50	18	58	26
63	55	47	39	31	23	15	7	33	1	41	9	49	17	57	25

2. Các khóa Ki được sinh ra từ khóa K ban đầu bằng cách hoán vị 56 bit để tạo

Alexa 2,500,293
Google Rank 0/10
RiseMyWeb

thành khóa 48 bit (hoặc hoán vị 64 bit để tạo thành khóa 56 bit):

57	49	41	33	25	17	9	14	17	11	24	1	5
1	58	50	42	34	26	18	3	28	15	6	21	10
10	2	59	51	43	35	27	23	19	12	4	26	8
19	11	3	60	52	44	36	16	7	27	20	13	2
63	55	47	39	31	23	15	41	52	31	37	47	55
7	62	54	46	38	30	22	30	40	51	45	33	48
14	6	61	53	45	37	29	44	49	39	56	34	53
21	13	5	28	20	12	4	46	42	50	36	29	32

3. Các bước để tính hàm $f(A, J) : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$

- o Tính $E(A)$ - mở rộng A từ 32 bit lên thành 48 bit:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

- o Tính $B = E(A) \oplus J = B_1B_2B_3B_4B_5B_6B_7B_8$

- o Tính $C = C_1C_2C_3C_4C_5C_6$

với $C_j = S_j(B_j) = S_j(r = b_1b_6, c = b_2b_3b_4b_5)$,

trong đó ta có S_1 là:

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

- o Tính $f(A, J) = P(C)$ với

$$P = \begin{pmatrix} 16 & 7 & 20 & 21 \\ 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 \\ 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 \\ 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 \\ 22 & 11 & 4 & 25 \end{pmatrix}$$

[Add new comment](#)

Tags: [Cryptography](#) [Exercise](#) [Practice](#)

Windows Server 2003 SDK

Blog - Technical

Written by [Thong D. Nguyen](#)

Thursday, 14 October 2010 03:14

Windows Server 2003 SDK is an update for VC++6. Though Microsoft has

How to make Blue Screen of Death (BSOD) with few clicks

Blog - Technical

Written by [Thong D. Nguyen](#)

Monday, 11 October 2010 04:50

www.rvvv.ac.th/mph

Sat 22 | 30Chance of Rain

Sun 23 | 32Chance of Rain

Mon 22 | 28Chance of Storm

Tue 23 | 28Chance of Storm

Newsletter

released VS2005, VS2008, VS2010, somebody might prefer VC++6 in building their products. Windows Server 2003 SDK is the final SDK which supports the old VS98. The download links are not public anymore, to get the SDK you have to purchase a CD from Microsoft site.

[Read more...](#) [Add new comment](#)

Tags: [2003](#) [Microsoft](#)
[Microsoft Sdk](#) [2003](#) [Sdk](#)

User Rating:  / 1

Poor Best

You can make blue screen of death with few clicks. You might want to do this as a prank 😊, or you need to save memory dump, or test your application if you are a developer. Microsoft included simple way to do this, you only need to enable it first.

[Read more...](#) [Add new comment](#)

Tags: [Bsod](#) [Core](#) [Dump](#) [Microsoft](#)

Doctoral Degree vs. PhD: What's the Difference?

Blog - Misc

Written by [Thong D. Nguyen](#)

Friday, 08 October 2010 10:24

User Rating:  / 1

Poor Best

Doctoral degrees tend to carry with them an almost mystical quality because many people do not understand how one earns a doctoral degree or who should get one. Learn all about the difference between a doctoral degree and a PhD and which one may be the right degree for you.

[Read more...](#) [Comments \(1\)](#)

Tags: [Degree](#) [Difference](#) [Doctor](#)
[Doctorate](#) [Phd](#)

How to: Convert Between Various String Types

Blog - Technical

Written by [Thong D. Nguyen](#)

Monday, 27 September 2010 09:41

This topic demonstrates how to convert various Visual C++ string types into other strings. The strings types that are covered

include `char*`, `wchar_t*`, `_bstr_t`, `CComBS*` and `System.String`. In all cases, a copy of the string is made when converted to the new type. Any changes made to the new string will not affect the original string, and vice versa.

Source: MSDN

[Read more...](#) [Add new comment](#)

Tags: [C Plus Plus](#) [C Plus Plus .Net](#)
[Char](#) [Convert](#) [String](#)
[System.String](#) [Wchar](#)

More Articles...

- [Tài liệu hướng dẫn thực hành](#)
- [Cubic Solution](#)
- [Advanced Serial Programming](#)
- [MODEM Communication](#)

Page 1 of 7

« Start Prev [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) Next End »

