



HELLO!

I am Khanh

I'm here for my network-programming project's
presentation :))

You can find me at HEDSPI, Hanoi University of Science &
Technology



XÂY DỰNG DỊCH VỤ MÃ HÓA VÀ GIẢI

MÃ VĂN BẢN SỬ DỤNG THUẬT TOÁN

BASE64



NỘI DUNG

- Thuật toán Base64
- Lập trình client/server



BASE64



Phân biệt giữa “encoding” và “encryption”

Encoding

Chuyển đổi bằng mã ký tự

ASCII, UTF8, UTF16, Shift-JIS,
Base64, ...

- ✗ Tạo ra dữ liệu phù hợp
- ✗ Không nhằm mục đích bảo mật thông tin

Encryption





Thuật toán - Bảng mã Base64

value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
char	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P

value	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
char	Q	R	S	T	U	V	W	X	Y	Z	a	b	c	d	e	f

value	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
char	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v

value	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
char	w	x	y	z	0	1	2	3	4	5	6	7	8	9	+	/



Thuật toán - Mã hóa từ ASCII => Base64

3 ký tự ascii (24-bit) => 4 ký tự Base64

Text content	M		a		n	
ASCII	77 (0x4D)		97 (0x61)		110 (0x6E)	
Bit pattern	0 1 0 0 1 1 0 1		0 1 1 0 0 0 0 1		0 1 1 0 1 1 1 0	
Index	19	22	5	46		
Base64 encoded	T	W	F	u		



Thuật toán - Mã hóa từ ASCII => Base64

2 ký tự ascii (24-bit) => 3 ký tự Base64 và '='

Text content	M		a		
ASCII	77 (0x4D)		97 (0x61)		0 (0x00)
Bit pattern	0 1 0 0 1 1 0 1		0 1 1 0 0 0 0 1		0 0 0 0 0 0 0 0
Index	19		22	4	0
Base64 encoded	T		W	E	=



Thuật toán - Mã hóa từ ASCII => Base64

1 ký tự ascii (24-bit) => 2 ký tự Base64 và '=='

Text content	M			
ASCII	77 (0x4D)		0 (0x00)	0 (0x00)
Bit pattern	0 1 0 0 1 1 0 1		0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Index	19	16	0	0
Base64 encoded	T	Q	=	=



Thuật toán - Giải mã từ Base64 => ASCII

4 ký tự Base64 => 3 ký tự ASCII

Text content	c	3	V	y
Base64	28	55	21	50
Bit pattern	0 1 1 1 0 0	1 1 0 1 1 1	0 1 0 1 0 1	1 1 0 0 1 0
Index	115	117	114	
ASCII	s	u	r	



Thuật toán - Giải mã từ Base64 => ASCII

3 ký tự Base64 và '=' => 2 ký tự ASCII

Text content	c	3	U	=
Base64	28	55	20	
Bit pattern	0 1 1 1 0 0	1 1 0 1 1 1	0 1 0 1 0 0	
Index	115		117	
ASCII	s		u	
			'0'	



Thuật toán - Giải mã từ Base64 => ASCII

3 ký tự Base64 và '=' => 2 ký tự ASCII

Text content	c	w	=	=
Base64	28	48		
Bit pattern	0 1 1 1 0 0	1 1 0 0 0 0		
Index	115			
ASCII	s	'\0'		'\0'

2.

Lập trình
client/server



CLIENT

- ✗ Chứa cấu trúc `sockaddr_in` của server để kết nối tới server
- ✗ Tạo socket:

```
cli_sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
```

- ✗ Kết nối tới server:

```
connect(cli_sock, (struct sockaddr*)&srv_addr, sizeof(srv_addr))
```

- ✗ Nhận input đường dẫn file, lệnh encode/decode từ người dùng
- ✗ Gửi tín hiệu encode/decode lên cho server => nhận lại tín hiệu báo đã nhận từ server



CLIENT

✕ Mở file

```
int fd = open(file_path, O_RDONLY);
```

✕ Gửi file ra cổng cli_sock:

```
sendfile(cli_sock, fd, &offset, stat_buf.st_size)
```

✕ Đóng file, kết thúc gửi file:

```
close(fd);
```

```
shutdown(cli_sock, SHUT_WR);
```

✕ Nhận file trả về từ server:

```
while ((len = recv(cli_sock, buffer, MAX_RECV_BUF, 0)) > 0)  
{fwrite(buffer, 1, len, fd_);}
```



SERVER

- ✗ Chứa cấu trúc `sockaddr_in` của server và của client
- ✗ Tạo socket:

```
listen_fd = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)
```

- ✗ Bind socket to port:

```
bind(listen_fd, (struct sockaddr*) &srv_addr, sizeof(srv_addr))
```

- ✗ Listen for client:

```
listen(listen_fd, LISTEN_ENQ)
```

- ✗ Accept client:

```
conn_fd = accept(listen_fd, (struct sockaddr*) &cli_addr, &cli_len)
```



SERVER

- ✗ Nhận tín hiệu mã hóa/giải mã từ client:

```
recv(conn_fd, cli_msg, MAX_RECV_BUF, 0)
```

- ✗ Trả lời với client là đã nhận được:

```
send(conn_fd, reply, sizeof(reply), 0)
```

- ✗ Nhận file gửi từ client:

```
while ((len = recv(conn_fd, buffer, MAX_RECV_BUF, 0)) > 0)  
{fwrite(buffer, 1, len, fd);}
```

- ✗ Mã hóa/giải mã file: `encode("srv_result.txt"); decode("srv_result.txt");`

- ✗ Gửi trả file kết quả về cho client:

```
sendfile(conn_fd, fd_, &offset, stat_buf.st_size)
```

- ✗ Đóng socket





Xin cảm ơn thầy và các bạn đã
lắng nghe!

