Radix-64 Conversion in PGP

Cunsheng Ding
Department of CSE
HKUST

PGP E-Mail Compatibility

Many electronic mail systems can only transmit blocks of ASCII text. This can cause a problem when sending encrypted data since ciphertext blocks might not correspond to ASCII characters which can be transmitted.

PGP overcomes this problem by using **radix-64 conversion**.

PGP E-Mail Compatibility: Example

- Suppose the email message is: new
- ASCII format: 01101110 01100101 01110111
- After encryption: 10010001 10011010 10001000
- The problem after encryption:
  - the three bytes do not represent any key board ASCII characters.
  - Most email systems cannot transmit and process such a piece of ciphertext.

Radix-64 Conversion

Suppose the text to be encrypted has been converted into binary using ASCII coding and encrypted to give a ciphertext stream of binary.

Radix-64 conversion maps arbitrary binary into printable characters as follows:

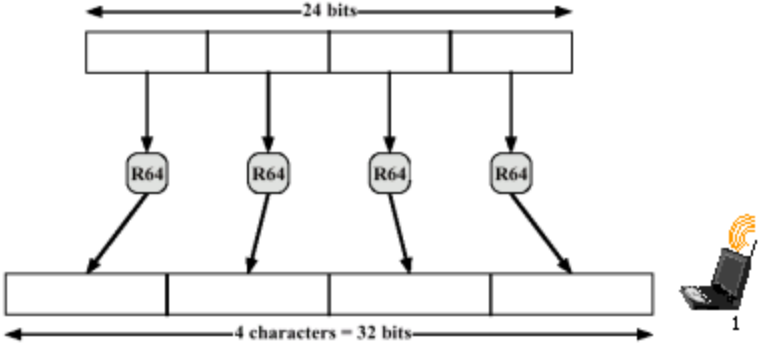
Radix-64 Conversion

1. The binary input is split into blocks of 24 bits (3 bytes).
2. Each 24 block is then split into four sets each of 6-bits.
3. Each 6-bit set will then have a value between 0 and 2^6-1 (=63).
4. This value is encoded into a printable character.

Pictorial Description

Radix-64 Conversion

- To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion
- Radix-64 expands a message by 33%



6 bit value	Character encoding	6 bit value	Character encoding	6 bit value	Character encoding	6 bit value	Character encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

Radix-64 Conversion: Example

- Suppose the email message is: new
- ASCII format: 01101110 01100101 01110111
- After encryption: 10010001 10011010 10001000
- The Radix-64 conversion:
  - The 24-bit block: 10010001 10011010 10001000
  - Four 6-bit blocks: 100100 011001 101010 001000
  - Integer version: 36 25 38 8
  - Printable version: k Z m I