转 openssl库中的BIGNUM

2012年11月20日 13:42:06 阅读数：7765

openssl库中的BIGNUM，处理大数比较好，可以用在很多方面。

BIGNUM是一个typedef的结构，可以直接使用。但一般来说，使用它的指针结构。如：BIGNUM *p;

BIGNUM的创建与释放

函数原型	解释	示例
BIGNUM * BN_new (void);	创建一个BIGNUM的结构，返回新BIGNUM结构的指针	BIGNUM *a = BN_new ();
void BN_free (BIGNUM *);	释放一个BIGNUM	free (a);

BIGNUM的值测试

函数原型	解释	示例
int BN_cmp (BIGNUM *a, BIGNUM *b);	| 判断a与b是否相等	if (BN_cmp (a, b) { printf ("a equ b/n"); }
<verbatim>int BN_ucmp (BIGNUM *a, BIGNUM *b);	判断a与b的绝对值是否相等	if (BN_ucmp (a, b)
int BN_is_zero(BIGNUM *a);	判断a是不是为0	if (BN_is_zero (a))
int BN_is_one(BIGNUM *a);	判断a是不是1	if (BN_is_one (a))
int BN_is_word(BIGNUM *a, BN_ULONG w);	判断a是不是值w	if (BN_is_word (a, 12))
int BN_is_odd(BIGNUM *a);	判断a是不是一个奇数	if (BN_is_odd (a))

BIGNUM的赋值与取值

函数原型	解释	示例
int BN_num_bytes(BIGNUM *a);	返回a的字节数	printf ("length: %d/n", BN_num_tytes (a));
int BN_num_bits(BIGNUM *a);	返回a的二进制位数	printf ("bits: %d/n", BN_num_bits (a));
int BN_one(BIGNUM *a);	设置a为1	BN_one (a);
int BN_zero(BIGNUM *a);	设置a为0	BN_zero (a);
int BN_bn2bin(const BIGNUM *a, unsigned char *to);	取a为二进制到to中，返回字符串长度	char s[1024]; int length = BN_bn2bin (a, s);
BIGNUM *BN_bin2bn(const unsigned char *s, int len, BIGNUM *ret);	赋二进制值s到ret中，返回ret	char s[] = "1001001"; BN_bin2bn (s, strlen (s), a);

char *BN_bn2hex(const BIGNUM *a);	取a的16进制值，返回一个字符串的指针。此指针要使用完后，手动使用OPENSSL_free释放	char *p = BN_bn2hex (a);
		if (p)
		{
		printf ("number is 0x%s/n", p);
		OPENSSL_free (p);
		}

char *BN_bn2dec(const BIGNUM *a);	取a的10进制值，返回一个字符串的指针。此指针要使用完后，手动使用OPENSSL_free释放	p = BN_bn2dec (a);
int BN_hex2bn(BIGNUM **a, const char *str);	赋16进制值str到*a中，返回成功与否	BN_hex2bn (&a, "0x123F23D12");
int BN_dec2bn(BIGNUM **a, const char *str);	赋10进制值str到*a中，返回成功与否	BN_dec2bn (&a, "1999");

BIGNUM的计算

函数原型	解释	示例
int BN_add(BIGNUM *r, const BIGNUM *a, const BIGNUM *b);	计算a与b的和，值储存在r中。如果成功，返回1；否则，返回0	BIGNUM *a = BN_new (), *b = BN_new (), *r = BN_new (); BN_dec2bn (&a, "1234"); BN_dec2bn (&b, "2345"); BN_add (r, a, b);
int BN_sub(BIGNUM *r, const BIGNUM *a, const BIGNUM *b);	计算a与b的差，值储存在r中。返回1或者0	BN_sum (r, a, b);
int BN_mul(BIGNUM *r, BIGNUM *a, BIGNUM *b, BN_CTX *ctx);	计算a与b的积，值储存在r中。返回1或者0。ctx为一个上下文相关的结构，可以用BN_CTX_new与BN_CTX_free来创建与释放它	BN_CTX *ctx = BN_CTX_new (); BN_mul (r, a, b, ctx); BN_CTX_free (ctx);
int BN_sqr(BIGNUM *r, BIGNUM *a, BN_CTX *ctx);	计算a的平方，值储存在r中。返回1或者0	BN_sqr (r, a, ctx);
int BN_div(BIGNUM *dv, BIGNUM *rem, const BIGNUM *a, const BIGNUM *d, BN_CTX *ctx);	计算a与d的商，值储存在dv中，余数储存在rem中。返回1或者0	BN_div (dv, r, a, b);
int BN_mod(BIGNUM *rem, const BIGNUM *a, const BIGNUM *m, BN_CTX *ctx);	计算a与m的模，值储存在rem中。返回1或者0	BN_mod (r, a, m, ctx);
int BN_nnmod(BIGNUM *r, const BIGNUM *a, const BIGNUM *m, BN_CTX *ctx);	计算a与m的模，并且结果如果小于0，就加上m，值储存在r中。返回1或者0	BN_nnmod (r, a, m, ctx);
int BN_mod_add(BIGNUM *r, BIGNUM *a, BIGNUM *b, const BIGNUM *m, BN_CTX *ctx);	计算a与b的和，再模m，值储存在r中。返回1或者0	BN_mod_add (r, a, b, m, ctx);
int BN_mod_sub(BIGNUM *r, BIGNUM *a, BIGNUM *b, const BIGNUM *m, BN_CTX *ctx);	计算a与b的差，再模m，值储存在r中。返回1或者0	BN_mod_sub (r, a, b, m, ctx);
int BN_mod_mul(BIGNUM *r, BIGNUM *a, BIGNUM *b, const BIGNUM *m, BN_CTX *ctx);	计算a与b的积，再模m，值储存在r中。返回1或者0	BN_mod_mul (r, a, b, m, ctx);
int BN_mod_sqr(BIGNUM *r, BIGNUM *a, const BIGNUM *m, BN_CTX *ctx);	计算a的平方根，再模m，值储存在r中。返回1或者0	BN_mod_sqr (r, a, m, ctx);
int BN_exp(BIGNUM *r, BIGNUM *a, BIGNUM *p, BN_CTX *ctx);	计算a的p次方，值储存在r中。返回1或者0	BN_exp (r, a, p, ctx);
int BN_mod_exp(BIGNUM *r, BIGNUM *a, const BIGNUM *p, const BIGNUM *m, BN_CTX *ctx);	计算a的p次方，再模m，值储存在r中。返回1或者0	BN_mod_exp (r, a, p, m, ctx);
int BN_gcd(BIGNUM *r, BIGNUM *a, BIGNUM *b, BN_CTX *ctx);	计算a与b的最大公约数，值储存在r中。返回1或者0	BN_gcd (r, a, b, ctx);
int BN_add_word(BIGNUM *a, BN_ULONG w);	大数a加上w，值储存在a中，返回1或者0	BN_dec2bn (a, "1234"); BN_add_word (a, 1);
int BN_sub_word(BIGNUM *a, BN_ULONG w);	大数a减去w，值储存在a中，返回1或者0	BN_sub_word (a, 23);
int BN_mul_word(BIGNUM *a, BN_ULONG w);	大数a乘以w，值储存在a中，返回1或者0	BN_mul_word (a, 2);
BN_ULONG BN_div_word(BIGNUM *a, BN_ULONG w);	大数a除以w，值储存在a中，返回余数	BN_ULONG ru = BN_div_word (a, 256);
BN_ULONG BN_mod_word(const BIGNUM *a, BN_ULONG w);	大数a模w，返回余数	ru = BN_mod_word (a, 256);

转自：http://blogold.chinaunix.net/u/19628/showart_2081074.html

个人分类：openssl ▼查看关于本篇文章更多信息

上一篇 信号量sem_t，互斥锁pthread_mutex_t的使用

下一篇 VS2010控制台程序运行一闪而过的完美解决办法