

۱۴۶.۳۸۷  
۵۵,۱۰۵

به نام خدا



مؤسسه فرهنگی هنری  
دیباگران تهران

# رمانگاری

مؤلف:

دکتر بهروز فرزندان

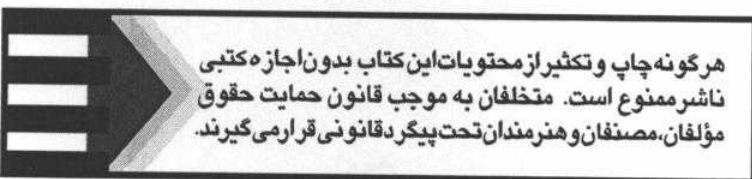
مترجمین:

مهندس ماحد شکری

کارشناس ارشد امنیت اطلاعات و مدرس دانشگاه

مهندس ابوالفضل یوسفی راد

کارشناس ارشد امنیت اطلاعات، دبیر آموزش و پرورش و مدرس دانشگاه



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی  
ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق  
مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

سرشناسه: فروزان، بهروز، ۱۳۲۳-

عنوان و نام پدید آور: رمزنگاری / مؤلف: بهروز  
فروزان؛ مترجمان: ماحد شکری، ابوالفضل یوسفی راد

مشخصات نشر: تهران- دیباگران تهران- ۱۳۹۵

مشخصات ظاهری: ۴۹۵ ص

شابک: ۹۷۸-۶۰۰-۱۲۴-۵۱۸-۳

وضعیت فهرست نویسی: قیفا

یادداشت: کتاب حاضر ترجمه گزیده ای از Cryptography  
and network security است.

موضوع: شبکه های کامپیوتری - تدابیر ایمنی

موضوع: Computer networks-security measures

موضوع: رمزنگاری

موضوع: Cryptography

شناسه افزود: شکری، ماحد، ۱۳۷۱-مترجم

شناسه ای: یوسفی راد، ابوالفضل، ۱۳۶۵-مترجم

رده بندی کنگره: ۰۱۱۳۰۰۴۳ / TK ۵۱۰۵ / ۵۹

رده بندی دیویی: ۵/۸

شماره کتابشناسی ملی: ۴۵۰۵۹۷۹

## Cryptography and: عنوان کتاب اصلی Network security

عنوان کتاب: رمزنگاری

مؤلف: دکتر بهروز فروزان

مترجمین: ماحد شکری - ابوالفضل یوسفی راد

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه آرایی: بهرام مزگانی سیرین

طرح روی جلد: مجتبی حجازی

چاپ: دانشجو

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۵

تیراژ: ۱۵۰ جلد

قیمت: ۵۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۵۱۸-۳

ISBN: 978-600-124-518-3

نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶ کد پستی: ۱۳۱۴۹۸۳۱۸۵

پست الکترونیکی: [bookmarket@mftmail.com](mailto:bookmarket@mftmail.com)

فروش اینترنتی:

[www.mftshop.com](http://www.mftshop.com)

[www.mftbook.ir](http://www.mftbook.ir)

نشانی اینستاگرام: Dibagaran\_publishing

نشانی تلگرام: @mftbook

## فهرست مطالب

|    |                                    |
|----|------------------------------------|
| ۱۵ | مقدمه مترجمان                      |
| ۱۷ | بخش اول                            |
| ۱۷ | مقدمه                              |
| ۱۷ | فصل اول                            |
| ۱۷ | مقدمه ای بر امنیت اطلاعات          |
| ۱۷ | اهدای فصل                          |
| ۱۹ | ۱،۱ الف امنیتی                     |
| ۱۹ | محرمانگی                           |
| ۲۰ | جامعیت                             |
| ۲۰ | در دسترس پذیری                     |
| ۲۰ | ۱،۲ حملات                          |
| ۲۱ | حملات علیه محرمانگی                |
| ۲۲ | حملات علیه جامعیت                  |
| ۲۴ | حملات علیه در دسترس پذیری          |
| ۲۴ | حملات فعال در مقابل حملات غیر فعال |
| ۲۶ | ۱،۳ سرویس ها و مکانیزم ها          |
| ۲۶ | سرویس های امنیتی                   |
| ۲۸ | مکانیزم های امنیتی                 |
| ۳۱ | رابطه بین سرویس ها و مکانیزم ها    |
| ۳۱ | ۱،۴ تکنیک ها                       |
| ۳۲ | رمزنگاری                           |
| ۳۳ | پنهان نگاری                        |

|    |                                 |
|----|---------------------------------|
| ۳۷ | ۱,۵ منابع پیشنهادی              |
| ۳۷ | کتاب ها                         |
| ۳۷ | وبسایت ها                       |
| ۳۷ | ۱,۶ عبارات کلیدی                |
| ۳۹ | ۱,۷ خلاصه                       |
| ۴۱ | بخش دوم                         |
| ۴۱ | رمزنگاری کلید متقارن            |
| ۴۱ | فصل دوم                         |
| ۴۱ | ریاضیات رمزنگاری                |
| ۴۱ | (حساب پیمانه ای هم آری ماتریس)  |
| ۴۲ | ۲,۱ حساب اعداد صحیح             |
| ۴۲ | مجموعه اعداد صحیح               |
| ۴۲ | عملیات دودویی                   |
| ۴۲ | تقسیم اعداد صحیح                |
| ۴۶ | تقسیم پذیری                     |
| ۵۴ | معادلات خطی دیوفانتین           |
| ۵۷ | ۲,۲ حساب پیمانه ای              |
| ۵۷ | عملگر پیمانه ای                 |
| ۵۹ | مجموعه باقیمانده ها: $Z_n$      |
| ۵۹ | هم ارزی                         |
| ۶۲ | عملیات در $Z_n$                 |
| ۶۷ | معکوس                           |
| ۷۳ | جداول جمع و ضرب                 |
| ۷۴ | مجموعه های مختلف برای جمع و ضرب |

|     |                           |
|-----|---------------------------|
| ۷۵  | دو مجموعه دیگر            |
| ۷۵  | ۲,۳ ماتریس                |
| ۷۶  | تعاریف                    |
| ۷۷  | عملیات و روابط            |
| ۷۹  | دترمینان                  |
| ۸۲  | ۲,۴ هم ارزی خطی           |
| ۸۳  | معادلات خطی تک - متغیره   |
| ۸۵  | مجموعه معادلات خطی        |
| ۸۶  | ۲,۵ منابع پیشین           |
| ۸۶  | کتاب ها                   |
| ۸۷  | وبسایت ها                 |
| ۸۷  | ۲,۶ عبارات کلیدی          |
| ۸۸  | ۲,۷ خلاصه                 |
| ۹۱  | فصل سوم                   |
| ۹۱  | رمزهای کلید متقارن سنتی   |
| ۹۱  | اهداف فصل                 |
| ۹۲  | ۳,۱ مقدمه                 |
| ۹۵  | اصل کیرشهف                |
| ۹۵  | تحلیل رمز                 |
| ۱۰۰ | گروه بندی رمزهای سنتی     |
| ۱۰۰ | ۳,۲ رمزهای جانشینی        |
| ۱۰۱ | رمزهای جانشینی تک الفبایی |
| ۱۱۲ | رمزهای جانشینی تک الفبایی |
| ۱۳۲ | ۳,۳ رمزهای جابجایی        |

|     |                                   |
|-----|-----------------------------------|
| ۱۳۲ | رمزهای جابجایی بدون کلید          |
| ۱۳۴ | رمزهای جابجایی کلید دار           |
| ۱۳۵ | ترکیب دو روش                      |
| ۱۴۳ | ۳،۴ رمزهای دنباله ای و بلوکی      |
| ۱۴۳ | رمزهای دنباله ای                  |
| ۱۴۵ | رمزهای بلوکی                      |
| ۱۴۶ | ترکیب                             |
| ۱۴۶ | ۳،۵ تبع پیشنهادی                  |
| ۱۴۷ | کتاب ها                           |
| ۱۴۷ | وبسایت ها                         |
| ۱۴۷ | ۳،۶ عبارات کلیدی                  |
| ۱۴۹ | ۳،۷ خلاصه                         |
| ۱۵۱ | فصل چهارم                         |
| ۱۵۱ | ریاضیات رمزنگاری (ساختارهای جبری) |
| ۱۵۲ | ۴،۱ ساختارهای جبری                |
| ۱۵۲ | گروه ها                           |
| ۱۶۳ | حلقه                              |
| ۱۶۵ | میدان                             |
| ۱۶۸ | خلاصه                             |
| ۱۶۸ | ۴،۲ میدان های $GF(2^n)$           |
| ۱۷۰ | چند جمله ای ها                    |
| ۱۸۱ | استفاده از مولد                   |
| ۱۸۴ | ۴،۳ منابع پیشنهادی                |
| ۱۸۴ | کتاب ها                           |

|     |                                     |
|-----|-------------------------------------|
| ۱۸۵ | وبسایت ها                           |
| ۱۸۵ | ۴,۴ عبارات کلیدی                    |
| ۱۸۶ | ۴,۵ خلاصه                           |
| ۱۸۹ | فصل پنجم                            |
| ۱۸۹ | مقدمه ای بر رمزهای کلید متقارن مدرن |
| ۱۹۰ | ۵,۱ رمزهای بلوکی مدرن               |
| ۱۹۲ | جانشینی یا جابجایی                  |
| ۱۹۹ | اجزای رمز بلوکی مدرن                |
| ۲۰۴ | S-Boxes                             |
| ۲۱۱ | رمزهای عمل                          |
| ۲۱۵ | دو کلاس از رمزهای عمل               |
| ۲۲۱ | حملات روی رمزهای بلوک               |
| ۲۲۹ | ۵,۲ رمزهای دنباله ای مدرن           |
| ۲۳۰ | رمزهای دنباله ای همزمان             |
| ۲۳۸ | رمزهای دنباله ای غیر همزمان         |
| ۲۳۸ | ۵,۳ منابع پیشنهادی                  |
| ۲۳۸ | کتاب ها                             |
| ۲۳۹ | وبسایت ها                           |
| ۲۳۹ | ۵,۴ عبارات کلیدی                    |
| ۲۴۱ | ۵,۵ خلاصه                           |
| ۲۴۵ | فصل ششم                             |
| ۲۴۵ | استاندارد رمزگذاری داده (DES)       |
| ۲۴۶ | ۶,۱ مقدمه                           |
| ۲۴۶ | تاریخچه                             |

|     |       |                                   |
|-----|-------|-----------------------------------|
| ۲۴۷ | ..... | مرور اجمالی                       |
| ۲۴۷ | ..... | ۶,۲ ساختار DES                    |
| ۲۴۸ | ..... | جایگشت های اولیه و نهایی          |
| ۲۵۱ | ..... | راند ها                           |
| ۲۵۸ | ..... | رمز و معکوس رمز                   |
| ۲۶۵ | ..... | مثال ها                           |
| ۲۶۷ | ..... | ۶,۳ تحلیل DES                     |
| ۲۶۸ | ..... | خصوصیات                           |
| ۲۶۹ | ..... | معیار های طراحی                   |
| ۲۷۱ | ..... | نقاط ضعف DES                      |
| ۲۷۸ | ..... | ۶,۴ DES چندگانه                   |
| ۲۸۰ | ..... | DES دوگانه                        |
| ۲۸۲ | ..... | DES سه گانه                       |
| ۲۸۴ | ..... | ۶,۵ امنیت DES                     |
| ۲۸۴ | ..... | حمله جستجوی فراگیر                |
| ۲۸۴ | ..... | تحلیل رمز تفاضلی                  |
| ۲۸۵ | ..... | تحلیل رمز خطی                     |
| ۲۸۵ | ..... | ۶,۶ منابع پیشنهادی                |
| ۲۸۵ | ..... | کتاب ها                           |
| ۲۸۵ | ..... | وبسایت ها                         |
| ۲۸۶ | ..... | ۶,۷ عبارات کلیدی                  |
| ۲۸۷ | ..... | ۶,۸ خلاصه                         |
| ۲۸۹ | ..... | فصل هفتم                          |
| ۲۸۹ | ..... | استاندارد رمز گذاری پیشرفته (AES) |



|     |                                 |
|-----|---------------------------------|
| ۲۹۰ | ۷,۱ مقدمه                       |
| ۲۹۰ | تاریخچه                         |
| ۲۹۱ | معیارها                         |
| ۲۹۱ | راندها                          |
| ۲۹۳ | واحدهای داده                    |
| ۲۹۶ | ساختار هر رانده                 |
| ۲۹۷ | ۷,۲ تبدیلات                     |
| ۲۹۸ | جانشین                          |
| ۳۰۴ | جایگشت                          |
| ۳۰۷ | مخلوط کردن                      |
| ۳۱۱ | اضافه کردن کلید                 |
| ۳۱۲ | ۷,۳ توسعه کلید                  |
| ۳۱۳ | توسعه کلید در AES-128           |
| ۳۱۹ | توسعه کلید در AES-192 و AES-256 |
| ۳۲۰ | تحلیل توسعه کلید                |
| ۳۲۰ | ۷,۴ رمزها                       |
| ۳۲۱ | طراحی اصلی                      |
| ۳۲۲ | طراحی ثانویه                    |
| ۳۲۵ | ۷,۵ مثال ها                     |
| ۳۲۸ | ۷,۶ تحلیل AES                   |
| ۳۲۸ | امنیت                           |
| ۳۲۹ | پیاده سازی                      |
| ۳۲۹ | سادگی و هزینه                   |
| ۳۳۰ | ۷,۷ منابع پیشنهادی              |

|     |                                                |
|-----|------------------------------------------------|
| ۳۳۰ | کتاب ها                                        |
| ۳۳۰ | وبسایت ها                                      |
| ۳۳۱ | ۷,۸ عبارات کلیدی                               |
| ۳۳۱ | ۷,۹ خلاصه                                      |
| ۳۳۵ | فصل هشتم                                       |
| ۳۳۵ | رمزگذاری با استفاده از رمزهای کلید متقارن مدرن |
| ۳۳۶ | ۸,۱ استفاده از رمزهای بلوکی مدرن               |
| ۳۳۶ | حالت کتابچه الکترونیکی (ECB)                   |
| ۳۴۰ | حالت زنجیره بلوک های رمز (CBC)                 |
| ۳۴۴ | حالت بازخورد رمز (CFB)                         |
| ۳۴۸ | حالت بازخورد خروجی (OCF)                       |
| ۳۵۱ | حالت شمارنده (CTR)                             |
| ۳۵۴ | ۸,۲ استفاده از رمزهای دنباله ای                |
| ۳۵۴ | RC4                                            |
| ۳۵۹ | A5/1                                           |
| ۳۶۴ | ۸,۳ مسائل دیگر                                 |
| ۳۶۴ | مدیریت کلید                                    |
| ۳۶۴ | تولید کلید                                     |
| ۳۶۵ | ۸,۴ منابع پیشنهادی                             |
| ۳۶۵ | کتاب ها                                        |
| ۳۶۵ | وبسایت ها                                      |
| ۳۶۶ | ۸,۵ عبارات کلیدی                               |
| ۳۶۶ | ۸,۶ خلاصه                                      |
| ۳۶۹ | بخش سوم                                        |

|     |                                                            |
|-----|------------------------------------------------------------|
| ۳۶۹ | ..... رمزنگاری کلید نامتقارن                               |
| ۳۶۹ | ..... فصل نهم                                              |
| ۳۶۹ | ..... ریاضیات رمزنگاری (اعداد اول و معادلات هم ارزی مرتبط) |
| ۳۷۰ | ..... ۹.۱ اعداد اول                                        |
| ۳۷۰ | ..... تعریف                                                |
| ۳۷۲ | ..... کاردینالیتی (مرتبه) اعداد اول                        |
| ۳۷۳ | ..... بررسی اول بودن                                       |
| ۳۷۵ | ..... نام فیبوناچی                                         |
| ۳۷۷ | ..... قضیه ک-جک                                            |
| ۳۸۰ | ..... قضیه اولر                                            |
| ۳۸۲ | ..... تولید اعداد اول                                      |
| ۳۸۴ | ..... ۹.۲ آزمون اول بودن                                   |
| ۳۸۴ | ..... الگوریتم های قطعی                                    |
| ۳۸۷ | ..... الگوریتم های احتمالی                                 |
| ۳۹۶ | ..... آزمون اول بودن پیشنهادی                              |
| ۳۹۷ | ..... ۹.۳ فاکتورگیری                                       |
| ۳۹۸ | ..... قضیه بنیادی حساب                                     |
| ۳۹۹ | ..... روش های فاکتورگیری                                   |
| ۴۰۱ | ..... روش فرما                                             |
| ۴۰۲ | ..... روش $p-1$ پولارد                                     |
| ۴۰۳ | ..... روش $\rho$ پولارد                                    |
| ۴۰۷ | ..... روش های کارآمدتر                                     |
| ۴۰۸ | ..... ۹.۴ قضیه باقیمانده چینی                              |
| ۴۱۱ | ..... کاربردها                                             |

|          |                                          |
|----------|------------------------------------------|
| ۴۱۱..... | ۹,۵ هم ارزی درجه دوم.....                |
| ۴۱۲..... | هم ارزی درجه دوم با پیمانه عدد اول.....  |
| ۴۱۵..... | هم ارزی درجه دوم با پیمانه عدد مرکب..... |
| ۴۱۶..... | ۹,۶ بتوان رسانی و لگاریتم.....           |
| ۴۱۶..... | بتوان رسانی.....                         |
| ۴۱۹..... | لگاریتم.....                             |
| ۴۲۷..... | ۹,۷ منابع : شتهادی.....                  |
| ۴۲۷..... | کتاب ها.....                             |
| ۴۲۸..... | وبسایت ها.....                           |
| ۴۲۸..... | ۹,۸ عبارات کلیدی.....                    |
| ۴۳۰..... | ۹,۹ خلاصه.....                           |
| ۴۳۳..... | فصل دهم.....                             |
| ۴۳۳..... | رمزنگاری کلید نامتقارن.....              |
| ۴۳۴..... | ۱۰,۱ مقدمه.....                          |
| ۴۳۵..... | کلیدها.....                              |
| ۴۳۵..... | ایده کلی.....                            |
| ۴۳۷..... | نیاز به هر دو.....                       |
| ۴۳۸..... | تابع یک طرفه درجه دار.....               |
| ۴۴۰..... | سیستم رمز کوله پشتی.....                 |
| ۴۴۵..... | ۱۰,۲ سیستم رمز RSA.....                  |
| ۴۴۵..... | مقدمه.....                               |
| ۴۴۶..... | رویه.....                                |
| ۴۵۰..... | تعدادی مثال آموزشی.....                  |
| ۴۵۲..... | حملات روی RSA.....                       |

|     |                                                |
|-----|------------------------------------------------|
| ۴۶۱ | پیشنهادهای                                     |
| ۴۶۱ | پدینگ بهینه رمزنگاری نامتقارن (OAEP)           |
| ۴۶۵ | کاربردها                                       |
| ۴۶۵ | ۱۰.۳ سیستم رمز رایین                           |
| ۴۶۶ | رویه                                           |
| ۴۶۹ | امنیت سیستم رایین                              |
| ۴۶۹ | ۱۰.۴ سیستم رمز الجمال                          |
| ۴۶۹ | سیستم رمز الجمال                               |
| ۴۷۰ | رویه                                           |
| ۴۷۱ | اثبات                                          |
| ۴۷۲ | تجزیه و تحلیل                                  |
| ۴۷۳ | امنیت الجمال                                   |
| ۴۷۵ | کاربرد                                         |
| ۴۷۵ | ۱۰.۵ سیستم رمز منحنی بیضوی                     |
| ۴۷۶ | منحنی بیضوی روی اعداد حقیقی                    |
| ۴۸۰ | منحنی بیضوی روی $GF(p)$                        |
| ۴۸۲ | منحنی بیضوی روی $GF(2^n)$                      |
| ۴۸۴ | شبیه سازی سیستم رمزنگاری الجمال با منحنی بیضوی |
| ۴۸۸ | ۱۰.۶ منابع پیشنهادی                            |
| ۴۸۸ | کتاب ها                                        |
| ۴۸۸ | وبسایت ها                                      |
| ۴۸۹ | ۱۰.۷ عبارات کلیدی                              |
| ۴۹۰ | ۱۰.۸ خلاصه                                     |
| ۴۹۴ | منابع                                          |

# خط‌مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی است که بتواند خواسته‌های به‌روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، برقرار واقع شویم.

گسترده‌گی علوم و تخصص‌های روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و رایج‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید. در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، نویسندگان، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود، با رفع کمبودها و نیازهای موجود، منابعی پربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت " آقایان مهندس ماحد شکری و مهندس ابوالفضل یوسفی راد از کارشناسان ارشد امنیت اطلاعات و مدرس دانشگاه " تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نمایم با مراجعه به آدرس [dibagaran.mft.info](mailto:dibagaran.mft.info) (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران

[Publishing@mftmail.com](mailto:Publishing@mftmail.com)

## مقدمه مترجمان

کتاب حاضر حاصل تلاش ها و تحقیقات پروفسور بهروز فروزان، استاد ممتاز دانشکده DeAnza کالیفرنیا است، که یکی از منابع اصلی در زمینه امنیت اطلاعات می باشد. عنوان اصلی کتاب "رمزنگاری و امنیت شبکه" است، اما تصمیم گرفتیم فقط مباحث مربوط به رمزنگاری اطلاعات را به عنوان یک کتاب جداگانه ترجمه کرده و جهت مطالعه در دسترس علاقمندان به این علم قرار دهیم.

کتاب ارائه شده بخش که شامل ۱۰ فصل می باشد، تشکیل شده است. بخش اول شامل معرفی، مقدمه ای بر امنیت اطلاعات، بخش دوم شامل ریاضیات و رمزهای کلید متقارن سنتی و مدرن، و بخش سوم شامل ریاضیات و رمزهای کلید نامتقارن می باشد.

کتاب پیشرو می تواند یک منبع ارزشگاهی یا یک منبع تخصصی برای مخاطبین حرفه ای در زمینه امنیت اطلاعات باشد. در واقع این کتاب می تواند به عنوان منبع درسی برای دانشجویان رشته های مرتبط همچون، مهندسی فناوری اطلاعات، مهندسی نرم افزار، علوم کامپیوتر و مهندسی برق در سطح کارشناسی و کارشناسی ارشد مورد استفاده قرار گیرد.

به یقین کتاب حاضر خالی از اشکال و خطا نیست. پس از خوانندگانی که ما را از این اشکالات و خطاها از طریق ناشر و یا پست های الکترونیک زیر مطلع می نمایند، نهایت تشکر و قدردانی را داریم.

ابوالفضل یوسفی راد  
usefirad@gmail.com

مادح شکری  
madeh.shokri@gmail.com