scenario attacks. Next, he shows how to handle cryptographic systems and protocols that are truly “fit for application”—and formally demonstrates their fitness. Mao presents practical examples throughout and provides all the mathematical background you’ll need. Coverage includes: Crytpo foundations, probability, information theory, computational complexity, number theory, algebraic techniques, and more. Authentication: basic techniques and principles vs. misconceptions and consequent attacks Evaluating real-world protocol standards including (PKI, SSL, TLS,G, and Kerberos) Designing stronger countermeasures to vulnerable “handshake” crypto schemes Maas introduces formal and reductionist methodologies to prove the “fitness-application” security of practical encryptions, signatures, signcryption, and authentication schemes. He gives detailed explanations for zero-knowledge protocols: definitions, zero-knowledge properties, equivalency vs. simulatability, argument vs. proof, round-efficiency, and non-interactive versions.

Visual Cryptography and Its Applications Jonathan Patrick Hicks 2011 ‘To this thesis, a number of new schemes are presented which address current problems and shortcomings within the area of visual cryptography. Visual cryptography provides a very powerful means by which a secret, in the form of a digital image, can be distributed (encoded) into two or more pieces known as shares. When these shares are viewed onto transparents and superimposed exactly together, the original secret can be recovered (decoded) without the necessity for computation. Traditionally, visual cryptography allows effective and efficient sharing of a single secret between a number of trusted parties. One aspect of the research within this thesis specifically addresses the issue of embedding more than two secrets within a set of two shares. Alignment poses a further problem. The placement of the shares must be specific. In order to ease alignment, the techniques developed within this thesis for sharing multiple secrets relaxes this restriction. The result is a scheme in which the shares can be superimposed upon one another in a multitude of positions and alignment styles which enables multiple secret recovery.

Applications of visual cryptography are also examined and presented. This is an area within visual cryptography that has had very little attention in terms of research. The primary focus of the work presented within this thesis concentrates on applications of visual cryptography in real world scenarios. For such a simple and effective method of sharing secrets, practical applications are as yet, limited. A number of novel uses for visual cryptography are presented that use theoretical techniques in a practical way.

Information Theory, Coding and Cryptography Ross Kang 2010 The fields of Information Theory, Coding and Cryptography are ever expanding, and the last six years have seen a spurt of new ideas germinate, mature and get absorbed in industrial standards and applications. Many of these new concepts have been added for this edition, including nine new sections and hundreds of new exercises, mostly non-routine. What else is new? New Chapters on measurement and analytic graph theory Supplementary exercises in each chapter -- ideal for reinforcing, reviewing, and testing. Solutions and hints, often illustrated with figures, to selected exercises -- nearly 50 pages worth. Reorganization and extensive revisions in more than half of the existing chapters for smoother flow of the exposition. Foreword: The first three chapters now preview a number of concepts, mostly via the exercises, to pique the interest of readers. Grass and Yellen take a comprehensive approach to graph theory that integrates careful exposition with exercises that address classical graph theory, operations research, data structures and algorithms, and algebra and topology.