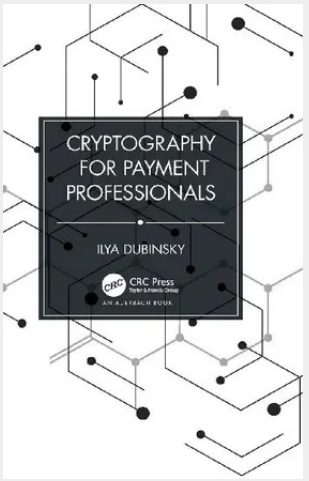
Dubinsky

Cryptography for Payment Professionals

Although cryptography plays an essential part in most modern solutions, especially in payments, cryptographic algorithms remain a black box for most users of these tools. Just as a sane backend developer does not drill down into low-level disk access details of a server filesystem, payments professionals have enough things to worry about before they ever need to bother themselves with debugging an encrypted value or a message digest. However, at a certain point, an engineer faces the need to identify a problem with a particular algorithm or, perhaps, to create a testing tool that would simulate a counterpart in a protocol that involves encryption. The world of cryptography has moved on with giant leaps. Available technical standards mention acronyms and link to more standards, some of which are very large while others are not available for free. After finding the standards for the algorithm, the specific mode of operation must also be identified. Most implementations use several cryptographic primitives—for example, key derivation with a block cipher, which produces a secret that is used together with a hash function and a double padding scheme to produce a digital signature of a base64-encoded value. Understanding this requires more sifting through online sources, more reading of platform and library documents, and finally, when some code can be written, there are very few test cases to validate it. Cryptography for Payment Professionals is intended for technical people, preferably with some background in software engineering, who may need to deal with a cryptographic algorithm in the payments realm. It does not cover the payment technology in-depth, nor does it provide more than a brief overview of some regulations and security standards. Instead, it focuses on the cryptographic aspects of each field it mentions. Highlights include: - Major cryptographic algorithms and the principles of their operation - Cryptographic aspects of card-present (e.g., magnetic stripe, EMV) and online (e.g., e-Commerce and 3DS 2.0) transactions - A detailed description of TDES DUKPT and AES DUKPT protocols, as well as an example implementation and test cases for both It is best if the reader understands programming, number and string representations in machine memory, and bit operations. Knowledge of C, Python, or Java may make the examples easier to read but this is not mandatory. Code related to the book is available at the author's GitHub site: https://github.com/ilya-dubinsky/cfpp



165,60 €
165,60 € (zzgl. MwSt.)

sofort versandfertig, Lieferfrist: 1-3 Werktage

Artikelnummer: 9781032442747
Medium: Buch
ISBN: 978-1-032-44274-7
Verlag: Auerbach Publications
Erscheinungstermin: 10.05.2023
Sprache(n): Englisch
Auflage: 1. Auflage 2023
Produktform: Gebunden
Gewicht: 476 g
Seiten: 204
Format (B x H): 161 x 240 mm