aut. Andrzej Kozłowski 14.09.2018

KRYPTOGRAFIA DLA KAŻDEGO [RECENZJA]

Kryptografia dla wielu wydaje się być bardzo skomplikowanym problemem, którego zgłębianie bez zaawansowanej znajomości matematyki jest niemożliwe. Jednocześnie jednak, coraz więcej osób szyfruje własne dane czy używa komunikatorów szyfrujących w technologii end-to-end. Dlatego też poznanie podstaw działania kryptografii wydaje się zasadne. Na polskim rynku przez długi okres czasu brakowało książki, która stanowiła prosty, praktyczny poradnik w tej dziedzinie. Sytuacja ta uległa jednak zmianie wraz z publikacją książki „Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania" Jeana-Philippe Aumassona wydana nakładem wydawnictwa PWN.

Autor Jean-Philippe Aumasson jest głównym inżynierem ds. badawczych w Kudelski Security, międzynarodowej firmie zajmującej się cyberbezpieczeństwem z siedzibą w Szwajcarii. Książka liczy sobie 304 strony, które składają się z 14 rozdziałów, wprowadzenia, skrótów oraz skorowidzu na samym końcu.

Pierwszy rozdział to w zasadzie wprowadzenie do tematyki. Autor omawia podstawy szyfrowania, sposób ich działania i bezpieczeństwo. To ostatnie szerzej jest poruszone w trzecim rozdziale. Czwarta i piąta część mówi odpowiednio o szyfrach blokowych i strumieniowych. Następne części książki poruszają taką problematyką jak RSA, protokoły Diffiego-Hellmana. Ostatni rozdział omawia tematykę kryptografii kwantowej i postkwantowej.

Książka może idealnie służyć jako podręcznik akademicki. Zawiera ona najważniejsze tematy związane z kryptografią. Do jej zalet zalicza się z pewnością przejrzystość prezentowanych zagadnień, dodatkowo wzbogaconych ilustracjami. Pisanie o tak trudnym temacie jakim jest kryptografia w sposób łatwy i zrozumiały jest wyjątkowo trudne. Aumassonowi to się jednak udaje. Szczególnie interesujący jest rozdział poświęcony kryptografii przyszłości, czyli kryptografii kwantowej i postkwantowej, która jeszcze nie istnieje, ale będzie miała potencjał do złamania całej wdrożonej kryptografii klucza publicznego i standardów.

Podsumowując, książka jest dobrym wprowadzeniem do skomplikowanego tematu kryptografii i robi to w sposób względnie łatwy. Autor nie unika podawania wzorów i równań, ale wyjaśnia ich znaczenie w bardzo przejrzysty sposób. Pracę Aumassona można polecić studentom kierunków informatycznych, osobom zawodowo pracującym z kryptografią na co dzień, jak również wszystkim zainteresowanym tym tematem