Supplemental Reading for The Future of Cryptanalysis

It’s been said that the advent of modern computing has spelled the death of the field of cryptanalysis; but the practice is still alive and well -- it’s the methodology that’s changed as technology has transformed the landscape. As quantum computing continues to develop, there’re concerns that modern encryption could be at risk of being broken. This is because most modern encryption algorithms are based on large prime number factorization being computationally difficult, something that can be significantly sped up by quantum computing. Because of this, quantum computing would allow for significantly faster factorization and brute-force attacks on encryption keys, making the future of modern cryptography questionable in the looming quantum computing era.