Zeszyty Naukowe
Wyższej Szkoły Ekonomii i Informatyki
Nr 20/2024, s. 161-174
DOI: XXXXXX

ISSN 1734-5391
e-ISSN 2957-2223

Zbigniew Handzel
Dr inż., prof. WSEI
Wyższa Szkoła Ekonomii i Informatyki
w Krakowie (WSEI)
email: zhandzel@wsei.edu.pl
ORCID: 0000-0003-1470-6592

Małgorzata Handzel
Mgr, Szkoła Podstawowa nr 164 w Krakowie

Mirosław Gajer
Dr inż. AGH Akademia Górniczo-Hutnicza
email:mgajer@wsei.edu.pl
ORCID: 0000-0003-3532-9482

WYZWANIA W ZAKRESIE CYBERBEZPIECZEŃSTWA W KONTEKŚCIE STALE ROSNĄCEJ LICZBY ZAGROŻEŃ I CYBERATAKÓW

CYBERSECURITY CHALLENGES IN THE CONTEXT OF AN INCREASING NUMBER OF THREATS AND CYBERATTACKS

Słowa kluczowe: *cyberbezpieczeństwo, cyberataki, cyberprzestępczość, kryptografia kwantowa*
Key words: *cybersecurity, cyberattacks, cybercrime, quantum cryptography*

JEL Classification: A2, C8, I2, L2, P4

Streszczenie

Problematyka cyberbezpieczeństwa jest obecnie jednym z najważniejszych wyzwań stojących przed ekspertami branży IT. Firmy, organizacje i inne jednostki borykają się z coraz większą liczbą zagrożeń, a cyberprzestępcy stosują coraz bardziej wyszukane metody ataków. Bezpieczeństwo informacji jest zatem priorytetowym zadaniem dla wszelkiego rodzaju instytucji oraz przedsiębiorstw. W pierwszej części niniejszego artykułu zostaną

omówione raporty dotyczące problematyki bezpieczeństwa cyfrowego oraz wyzwania stawiane systemom informatycznym w organizacjach i firmach, natomiast w części drugiej autorzy postarają się pokazać rolę algorytmów szyfrujących w dziedzinie cyberbezpieczeństwa oraz możliwości wykorzystania kryptografii kwantowej, jako obecnie najbardziej perspektywicznego rozwiązania, które można wykorzystać w procesie zabezpieczenia systemów IT.

Abstract
The issue of cyber security is currently one of the most important challenges facing IT experts. Companies, organizations and other entities are facing an increasing number of threats, and cyber criminals are using increasingly sophisticated methods of attack. Information security is therefore a priority task for all kinds of institutions and businesses. In the first part of this article, reports on digital security issues and challenges to information systems in organizations and companies will be discussed, while in the second part, the authors will try to show the role of encryption algorithms in the field of cyber security and the possibilities of using quantum cryptography, as currently the most promising solution that can be used in the process of securing IT systems.

WPROWADZENIE

Powszechna cyfryzacja i dynamiczny rozwój systemów informatycznych spowodował, iż cyberbezpieczeństwo stało się jednym z najważniejszych problemów współczesnych firm, organizacji, rządów i jednostek. Bezpieczeństwo informacji jest zatem priorytetowym zadaniem dla przedsiębiorstw, szczególnie w odniesieniu do danych strategicznych dla ich działalności. Transformacja cyfrowa spowodowała, iż odpowiednie zabezpieczenie danych i informacji stało się kluczowe. Należy pamiętać, iż ilość przetwarzanych informacji stale wzrasta, a wraz z nią liczba i złożoność zagrożeń. Im więcej zasobów do ochrony, tym więcej możliwości do nadużyć [1]. Z tego też powodu z roku na rok systematycznie wzrasta liczba zagrożeń oraz cyberataków, a rok 2023, w którym zanotowano znaczący wzrost cyberprzestępczości był pod tym względem rekordowy. Z raportu pełnomocnika rządu ds. cyberbezpieczeństwa wynika, że w porównaniu z poprzednim rokiem, w 2023 r. odnotowano ponad 100-procentowy wzrost cyberataków [2]. Z raportu Agencji Unii Europejskiej ds.

Cyberbezpieczeństwa ENISA z 2023 roku dotyczącego tzw. krajobrazu cyberbezpieczeństwa można dowiedzieć się o ujawnieniu ogromnej liczby zarejestrowanych incydentów, wynoszącej około 2580 wspomnianych incydentów między lipcem 2022 a czerwcem 2023 roku. W omawianym raporcie podkreślono główne zagrożenia, które opanowały krajobraz cyberbezpieczeństwa UE. Są to zagrożenia typu ransomware, znane z paraliżujących działań szyfrujących i taktyk wymuszania oraz zagrożenia związane z dostępnością istotnych usług i systemów mających znaczenie dla ciągłości funkcjonowania operacji cyfrowych. Ponadto problemem jest pojawienie się chatbotów opartych na sztucznej inteligencji [3]. Wszystko to stawia zatem nowe wyzwania przed specjalistami z zakresu bezpieczeństwa systemów informatycznych. Niniejszy artykuł ma na celu omówienie tych wyzwań, a autorzy postanowili dokonać analizy dostępnych raportów, pokazując zarówno problemy bezpieczeństwa jak też wyzwania i rekomendacje w tym zakresie.

ANALIZA WYBRANYCH RAPORTÓW DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA

Chcąc odpowiedzieć na pytanie dotyczące wyzwań w zakresie cyberbezpieczeństwa w kontekście stale rosnącej liczby zagrożeń i cyberataków należy dokonać analizy raportów przygotowanych przez ekspertów cyberbezpieczeństwa. Oczywiście dostępnych jest wiele takich raportów, natomiast na potrzeby niniejszego artykułu jego autorzy dokonali wyboru kilku raportów, opracowanych dla takich organizacji, jak Agencja Unii Europejskiej oraz Światowe Forum Ekonomiczne. Na początek autorzy niniejszego artykułu dokonali analizy raportu Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ENISA z 2023 roku. Ze wspomnianego raportu wynika, iż sektorem, który najczęściej jest ofiarą cyberataków jest administracja publiczna. Ten kluczowy sektor zmaga się z największą liczbą incydentów, co stawia pod znakiem zapytania bezpieczeństwo wrażliwych danych rządowych. Twórcy raportu podkreślają, że słabe punkty jednego sektora mogą szybko kumulować się oraz jednocześnie wpływać na wiele innych, tworząc efekt tzw. domina zakłóceń. Jak już wspomniano we wstępie, w omawianym raporcie podkreślono główne zagrożenia cyberbezpieczeństwa UE, którymi są: zagrożenia typu ransomware, znane z paraliżujących działań szyfrujących i taktyk wymuszania oraz zagrożenia związane z dostępnością istotnych usług [3]. Warto jednak zauważyć, iż

obok tak poważnych zagrożeń jak ransomware oraz zagrożeń związanych z dostępnością niezwykle poważnym problemem, a zarazem wyzwaniem dla specjalistów z zakresu cyberbezpieczeństwa jest pojawienie się chatbotów opartych na sztucznej inteligencji. Omawiany raport ENISA ujawnia wzrost chatbotów opartych na AI, wpływających na sytuację zagrożeń w cyberbezpieczeństwie. Wspomniane chatboty, choć wykorzystujące AI, stały się znane ze swoich zdolności do wprowadzania zakłóceń w funkcjonowaniu systemów IT, co niestety daje im znaczące miejsce wśród zagrożeń cybernetycznych [3]. Raport ENISA szczególnie podkreśla powszechność fałszywych informacji, czyli tzw. „fejków" oraz manipulacji informacjami z wykorzystaniem sztucznej inteligencji (AI) w celu wzniecania niepokoju, czy też wpływania na różnego rodzaju działalność. Jak słusznie zauważają twórcy raportu, chatboty oparte na AI, wyposażone są w zaawansowane algorytmy i uczenie maszynowe, co pozwala im naśladować interakcje ludzkie i szerzyć dezinformację i to w dodatku z bardzo dużą efektywnością. Wzrost liczby chatbotów opartych na AI stwarza unikalne wyzwania w zakresie cyberbezpieczeństwa. Tradycyjne mechanizmy obrony niestety mogą mieć trudności w zetknięciu się z tego typu zagrożeniami. Zapewnienie integralności danych, prywatności i bezpieczeństwa w erze sztucznej inteligencji staje się zatem ogromnym wyzwaniem [3].

Drugim analizowanym w niniejszym artykule raportem jest Raport Światowego Forum Ekonomicznego na temat globalnych perspektyw cyberbezpieczeństwa na 2023 rok „Global Cybersecurity Outlook 2023" [4]. Autorzy wspomnianego raportu: Paolo Dal Cin (Global Lead, Accenture Security) oraz Jeremy Jurgens (Managing Director, World Economic Forum) skupili się na rosnących wyzwaniach w zakresie cyberbezpieczeństwa, które wynikają z niestabilności geopolitycznej, szybkiego rozwoju technologii, niedoborów specjalistów oraz rosnących oczekiwań ze strony akcjonariuszy i regulatorów. Jako kluczowe punkty raportu autorzy wymieniają: niestabilność geopolityczną, nowe technologie wraz z nowymi zagrożeniami, zmiany regulacji prawnych, czy też rosnącą świadomość liderów biznesowych na temat cyberzagrożeń oraz niedobór wykwalifikowanych specjalistów w dziedzinie cyberbezpieczeństwa. Warto zauważyć, iż podobnie jak to miało miejsce w poprzednim raporcie, również tutaj szczególną uwagę zwraca się na zagrożenia typu ransomware, które zdaniem autorów omawianego raportu pozostaje jednym z najbardziej niepokojących zagrożeń, włącznie z atakami paraliżującymi działalność organizacji. Ponadto tutaj również zwrócono uwagę na zagrożenia związane z dostępnością krytycznych usług oraz na te wynikające z pojawie-

nia się chatbotów opartych na sztucznej inteligencji [4]. Ponadto autorzy omawianego raportu zwracają uwagę na związek pomiędzy napięciami geopolitycznymi a wzrostem liczby cyberzagrożeń. Z przedstawionych w raporcie wyników badań wynika, że aż 91% respondentów uważa, że w ciągu najbliższych dwóch lat prawdopodobne jest wystąpienie dalekosiężnego, katastrofalnego cyberataku. Ta rosnąca świadomość w zakresie cyberzagrożeń spowodowała, iż coraz częściej organizacje dostosowują swoje strategie cyberbezpieczeństwa, wzmacniając kontrolę nad stronami trzecimi i ponownie oceniając kraje, z którymi prowadzą działalność. Jednocześnie coraz częściej w strategii cyberbezpieczeństwa wykorzystuje się nowe technologie, tj.: sztuczną inteligencję, uczenie maszynowe i technologia chmurowa. Jednak ich integracja z istniejącymi systemami zwiększa złożoność i ryzyko [4]. Organizacje muszą zatem zrównoważyć wartość nowych technologii z potencjalnym ryzykiem cyberzagrożeń, co stanowi niemałe wyzwanie. Twórcy raportu zauważają ponadto, iż cyberprzestępczość staje się coraz bardziej profesjonalna, a grupy cyberprzestępcze koncentrują się na tworzeniu nowych typów ataków, dynamiczna zmienność zagrożeń utrudnia strategiczne planowanie obrony. Warto zauważyć również, iż ataki cyberprzestępców mają coraz częściej charakter systemowy, wpływając na całe sektory gospodarki, co z kolei zmusza organizacje do ciągłego monitorowania i oceny informacji o zagrożeniach. Coraz więcej ekspertów z zakresu cyberbezpieczeństwa uważa, że skutecznym narzędziem redukcji ryzyka są odpowiednie regulacje, które pomogą przesunąć zasoby prywatnego sektora w kierunku działań na rzecz cyberodporności. Chociaż uzyskanie zgodności z regulacjami może być nieco trudne, to jednak jest to konieczne do skutecznego zarządzania ryzykiem cybernetycznym [4]. Warto przy okazji zauważyć, iż wzrasta świadomość liderów biznesowych na temat cyberzagrożeń, a to prowadzi do lepszej integracji cyberbezpieczeństwa w strategiach zarządzania ryzykiem. Eksperci z zakresu cyberbezpieczeństwa coraz częściej spotkają się z zarządami firm, pomagając im w zrozumieniu i zarządzaniu ryzykiem cybernetycznym. Dzięki temu wspomniane zarządy firm i instytucji są świadome, że bezpieczeństwo ich organizacji zależy od zabezpieczeń stosowanych przez ich partnerów handlowych i dostawców. Organizacje stale wzmacniają zatem kontrolę nad stronami trzecimi, które mają dostęp do ich środowisk i danych. Niestety głównym problemem w zakresie zapewnienia bezpieczeństwa informatycznego jest niedobór wykwalifikowanych specjalistów z tego zakresu. Niezwykle ważnym zadaniem jest zatem stałe rozwijanie wiedzy i umiejętności zarówno specjalistów IT jak też innych pracowni-

ków w poszczególnych organizacjach. Organizacje powinny inwestować w szkolenia i rozwój pracowników, aby zwiększyć ich świadomość na temat zagrożeń i poprawić umiejętności reagowania na incydenty. W tym zakresie konieczne jest stworzenie programów szkoleniowych i staży, które umożliwią zdobycie umiejętności niezbędnych do zarządzania ryzykiem cybernetycznym [4]. Z omawianego raportu ENISA wynikają następujące rekomendacje:

- Poprawa Komunikacji – liderzy w zakresie cyberbezpieczeństwa powinni prezentować problemy związane z bezpieczeństwem cyfrowym w sposób zrozumiały dla liderów biznesowych, używając języka wspólnego i zrozumiałych metryk.
- Regularne Spotkania – częstsze spotkania pomiędzy ekspertami z zakresu cyberbezpieczeństwa a zarządami organizacji mogą znacząco pomóc w lepszym zrozumieniu ryzyka i priorytetów.
- Wzmocnienie Kultury Bezpieczeństwa – zwiększenie świadomości pracowników na temat cyberzagrożeń jest kluczowe dla budowania kultury bezpieczeństwa w organizacji.
- Zaangażowanie Zarządu – zdaniem autorów raportu zarządy powinny aktywnie wspierać inicjatywy na rzecz cyberbezpieczeństwa i włączać je w strategię biznesową.
- Inwestycje w Edukację – zdecydowanie należy inwestować w programy edukacyjne i szkoleniowe, które umożliwią rozwój umiejętności potrzebnych do zarządzania cyberzagrożeniami.

Trzecim wybranym do analizy raportem jest inny z przygotowanych przez ekspertów Światowego Forum Ekonomicznego, ale tym razem dotyczący Azji: „Global Cybersecurity Outlook 2023 – Southeast Asia". Przedstawione w raporcie badanie objęło 117 liderów cyberbezpieczeństwa z 32 krajów i 22 branż, przeprowadzone we współpracy z Accenture. Podobnie jak w przypadku wcześniej przedstawionego raportu, tutaj również jako jeden z głównych problemów bezpieczeństwa cyfrowego w Azji wskazano na geopolityczną niestabilność, która znacząco wpłynęła na postrzeganie strategii cyberbezpieczeństwa. Także w tym raporcie dużo uwagi poświęcono nowym technologiom, tj.: sztucznej inteligencji i uczeniu maszynowemu, które mają największy wpływ na strategie zarządzania ryzykiem cybernetycznym [5]. Eksperci z zakresu cyberbezpieczeństwa wskazali, że sztuczna inteligencja i uczenie maszynowe, większe zastosowanie technologii chmurowych oraz postępy w zarządzaniu tożsamością i dostępem użytkowników będą miały największy wpływ na ich strategie w ciągu najbliższych dwóch lat. Organizacje muszą inwestować w technologie, szkolenia i strategie, aby zwiększyć

swoją odporność na cyberataki. Współpraca między liderami biznesu, a liderami cyberbezpieczeństwa jest kluczowa dla skutecznego zarządzania ryzykiem i budowania długoterminowej odporności cybernetycznej [5].

Podsumowując raporty „Global Cybersecurity Outlook 2023", można zauważyć, iż eksperci przygotowujący w/w raporty podkreślają rosnące znaczenie cyberbezpieczeństwa w kontekście globalnych zagrożeń i niestabilności geopolitycznej. Wyzwaniem jest dynamicznie zmieniający się krajobraz zagrożeń cybernetycznych, w którym pojawia się coraz więcej profesjonalnych grup cyberprzestępczych, tworzących coraz więcej nowych typów ataków. Warto podkreślić również, iż implementacja nowych technologii w połączeniu z istniejącymi systemami zwiększa złożoność środowiska cyfrowego organizacji, co wymaga zarządzania ryzykiem cybernetycznym na wszystkich etapach procesu transformacji cyfrowej. Wzrost różnorodności ataków i ich systemowe skutki skłaniają organizacje do częstszego monitorowania i oceny zagrożeń, skracając cykle z rocznych na kwartalne, co obciąża zasoby cyberbezpieczeństwa. Specjaliści z zakresu cyberbezpieczeństwa podkreślają, że organizacje muszą inwestować w technologie, szkolenia i strategie, które zwiększą ich odporność na cyberataki. Kluczowe jest również wzmocnienie komunikacji między ekspertami cyberbezpieczeństwa, a zarządami firm, aby skutecznie zarządzać ryzykiem i budować długoterminową cyberodporność [4],[5].

WYZWANIA STAWIANE SYSTEMOM INFORMATYCZNYM W ORGANIZACJACH

Jak wynika z poprzedniego punktu, dynamiczny rozwój systemów informatycznych wraz ze wzrostem znaczenia w tych systemach AI, stawia przed specjalistami z zakresu cyberbezpieczeństwa coraz to nowe wyzwania. Krajobraz zagrożeń cybernetycznych zmienia się niezwykle dynamicznie, a coraz bardziej profesjonalnie działające grupy cyberprzestępcze stale rosną i tworzą coraz większą liczbę nowych typów ataków. Wzrost różnorodności ataków i coraz poważniejsze ich skutki, zmuszają organizacje do częstszego monitorowania i oceny zagrożeń, co w efekcie mocno obciąża zasoby cyberbezpieczeństwa. Zarządzanie bezpieczeństwem systemów informatycznych, w tym bezpieczeństwem przetwarzanych danych, staje się zatem coraz bardziej skomplikowane, a wraz tym coraz większe stają się oczekiwania wobec specjalistów bezpieczeństwa IT. Aby prawidłowo zarządzać bezpieczeństwem systemów informatycznych kluczowe jest

właściwe opracowanie tzw. polityki bezpieczeństwa organizacji. Dokument ten musi zostać opracowany w taki sposób, by możliwa była jego pełna implementacja, a w przyszłości aby można było w łatwy i szybki sposób uzupełniać oraz korygować poszczególne elementy omawianej polityki bezpieczeństwa. Niezwykle istotne jest w tym kontekście strategiczne podejście do problematyki zarządzania ryzykiem. Organizacje muszą pamiętać, że należy integrować zarządzanie ryzykiem cybernetycznym we wszystkich częściach działalności, takich jak planowanie ciągłości działania, finanse i rozwój produktów. Ponadto konieczna jest większa współpraca między liderami biznesu a liderami cyberbezpieczeństwa, aby mogli oni w wystarczającym stopniu zrozumieć specyfikę poszczególnych zagrożeń cybernetycznych i odpowiednio na nie reagować. Ustanowione regulacje muszą być postrzegane jako kluczowy element wpływający na odporność cybernetyczną organizacji ze względu na to, iż efektywne egzekwowanie regulacji może podnieść jakość cyberbezpieczeństwa w całym sektorze jak również w łańcuchach dostaw.

ROLA ALGORYTMÓW SZYFRUJĄCYCH

Niebagatelną rolę w ochronie danych przed niepowołanym dostępem pełnią algorytmy szyfrujące. Pierwotnie wszystkie algorytmy szyfrujące, przesyłane dane oparte były jedynie na koncepcji klucza symetrycznego, tzn. ten sam klucz wykorzystywany był zarówno do zaszyfrowania danych, jak i do ich deszyfracji. Pierwszy standard algorytmu szyfrującego opartego na koncepcji klucza symetrycznego został ustanowiony w USA w 1975 roku. Algorytm ten opierał swe działanie na kluczu 56-bitowym, przy czym pierwotne zakładano, że długość klucza szyfrującego miała wynosić aż 128 bitów, co zapewniałoby zdecydowanie wyższy poziom bezpieczeństwa rozważanego algorytmu, gdyż przy dostępnych wówczas mocach obliczeniowych byłby on w zasadzie niemożliwy do złamania w jakimkolwiek rozsądnym horyzoncie czasowym. Długość klucza szyfrującego została jednak ustawowo ograniczona, aby amerykańskie agencje rządowe miały przy pomocy ówcześnie istniejących superkomputerów możliwość złamania tego szyfru w sytuacji, gdyby zachodziło podejrzenie, że w grę może wchodzić poważne zagrożenie dla instytucji państwa, przykładowo ze strony grup przestępczych bądź organizacji terrorystycznych.

Takie postawienie sprawy spowodowało, że wielu badaczy zaczęło poszukiwać innego sposobu zapewniania obywatelom USA prywatności ich

korespondencji. W ten sposób narodziła się idea szyfrowania asymetrycznego. W przypadku tego rodzaju szyfrowania mamy do czynienia z dwoma rodzajami klucza szyfrującego. Pierwszy z nich jest ogólnie dostępny, co na pierwszy rzut oka może wydawać się wręcz swego rodzaju niedorzecznością, natomiast drugi jest tajny i w związku z tym przypisany jest tylko i wyłącznie do konkretnej osoby, do której falę, która spełnia równanie Schroedingera ma zostać wysłany szyfrogram. Zatem, jeśli coś chcemy wysłać zaszyfrowanego do pewnej osoby, to szyfrujemy to przy pomocy ogólnie dostępnego jej klucza publicznego i z tego powodu tylko i wyłącznie rozważana osoba jest w stanie to odszyfrować, korzystając w tym celu z własnego klucza prywatnego, którego nie wolno jej pod żadnym pozorem nikomu innemu ujawnić.

Warto zauważyć, że idea szyfrowania asymetrycznego rozwiązała także problem trudnego zagadnienia bezpiecznej dystrybucji klucza szyfrującego do osoby mającej odczytać szyfrogram, co ma miejsce w przypadku algorytmów z kluczem symetrycznym.

Idea szyfrowania asymetrycznego oparta jest na funkcji jednokierunkowej, tzn. takiej, której wartość zawsze może zostać wyznaczona w stosunkowo krótkim czasie dla dowolnego argumentu, natomiast wyznaczenie funkcji do niej odwrotnej, nawet za pomocą komputerów o największej mocy obliczeniowej, jest niemożliwe w czasie krótszym od co najmniej czasu istnienia wszechświata (13,7 miliarda lat) i właśnie na tym fakcie oparte jest bezpieczeństwo rozpatrywanego algorytmu szyfrującego.

Genialnym pomysłem było wykorzystanie w tym celu liczb pierwszych, ponieważ wyznaczenie ich iloczynu jest zawsze zadaniem relatywnie prostym do wykonania, natomiast jeśli dany jest już ten iloczyn i mielibyśmy teraz powiedzieć, jakie liczby pierwsze go tworzą, to jest to zagadnienie algorytmiczne, którego nie jesteśmy w stanie rozwiązać w czasie wielomianowym, ponieważ odpowiedniego algorytmu przeznaczanego do faktoryzacji liczby o wielomianowej złożoności obliczeniowej po prostu nie znamy. Z drugiej strony nikt jeszcze nie wykazał, że taki algorytm nie istnieje. Zatem, gdyby kiedyś w przyszłości został jednak odkryty wielomianowy algorytm faktoryzacji liczb, to omawiany sposób szyfrowania byłby wtedy już całkowicie bezużyteczny. Rozważany algorytm szyfrowania został określony skrótem RSA, pochodzącym od nazwisk jego twórców: Rives, Shamir, Adleman.

Oczywiście wykorzystywane w przypadku algorytmu RSA liczby pierwsze muszą być bardzo duże, przykładowo mogą mieć w zapisie binarnym nawet 2048 bitów. Zatem iloczyn dwóch takich liczb (p, q) będzie

miał długość 4096 bitów, co sprawia, że dokonanie jego faktoryzacji w jakimś rozsądnym przedziale czasowym jest praktycznie niewykonalne i to nawet przy zastosowaniu najszybszych obecnie superkomputerów. Oczywiście, jeśli w przyszłości moce obliczeniowe superkomputerów istotnie wzrosną, to stosowane w algorytmie RSA liczby pierwsze będą musiały być znacznie większe. Przykładowo będą mogły mieć w zapisie binarnym nawet 8192 bity bądź jeszcze więcej.

Tego rodzaju liczby generowane są w sposób losowy, co polega na tym, że najmłodszy bit ustawiany jest zawsze na jedynkę, a pozostałe bity są zerami bądź jedynkami losowanymi z równym prawdopodobieństwem. Oczywiście wygenerowana w ten sposób liczba najczęściej w ogóle nie jest liczbą pierwszą, ponieważ liczby pierwsze na osi liczbowej są rozmieszczone stosunkowo rzadko, a do tego ich dystrybucja wydaje się być całkowicie nieregularna, przy czym do chwili obecnej nie jest znany żaden wzór algebraiczny, który pozwalałby na wyliczenie wartości kolejnych liczb pierwszych.

Być może jednak chaos związany z rozmieszczeniem na osi liczbowej kolejnych liczb pierwszych jest jedynie pozorny i jest li tylko skutkiem swego rodzaju niedoskonałości ludzkiego umysłu, który nie jest w stanie dopatrzyć się w tym wypadku istniejącego tam mimo wszystko porządku – przesłanką ku temu jest tak zwana „spirala Ulama" utworzona z liczb naturalnych, odkryta przypadkowo przez polskiego matematyka Stanisława Ulama, która wyraźnie sugeruje, że jednak w królestwie liczb pierwszych panuje swego rodzaju porządek, a ich dystrybucja na osi liczbowej podlega jakimś nieznanym nam dotychczas regułom. Być może światło na te sprawy rzuciłoby udowodnienie postawionej w 1859 roku przez Bertranda Riemanna hipotezy dotyczącej rozmieszczenia na płaszczyźnie zespolonej tzw. nietrywialnych zer zdefiniowanej przez niego specjalnej funkcji dzeta. Niestety, po dziś dzień hipoteza Riemanna pozostaje już od ponad półtora wieku nadal nieudowodniona.

Powracając do głównego wątku naszych rozważań należy w jakiś sposób stwierdzić, czy wygenerowana w opisany, losowy sposób 2048-bitowa liczba jest liczbą pierwszą. W tym celu należałoby ją dzielić po kolei przez wszystkie liczby nieparzyste mniejsze od pierwiastka z tej liczby, jednak gdybyśmy chcieli postępować w ten sposób, to pracowalibyśmy dosłownie do końca świata. Inne, nieco szybsze metody, jak choćby sito Eratostenesa, też nie zdałyby się w tym wypadku na nic, po prostu tego rodzaju liczby są dla nich zbyt wielkie.

Musimy zatem poprzestać w rozważanym przypadku jedynie na prawdopodobieństwie, tzn. przyjmujemy z góry pewną wartość progową

prawdopodobieństwa (na przykład jedną miliardową) i w związku z tym godzimy się, że z takim właśnie prawdopodobieństwem (jak przykładowo jeden do miliarda) możemy od czasu do czasu przepuścić przez nasze sito jakąś liczbę złożoną, którą błędnie potraktujemy jako liczbę pierwszą. Od przyjętej przez nas wartości prawdopodobieństwa zależała będzie także liczba testów statystycznych pierwszości, które musimy obowiązkowo wykonać. Przykładowo w przypadku tzw. testu pierwszości Solvaya-Strassena prawdopodobieństwo przepuszczenia liczby złożonej jako liczby pierwszej wynosi jedna druga. Zatem jeśli omawiany test wykonamy przykładowo dziesięciokrotnie, to prawdopodobieństwo przepuszczenia liczby złożonej jako liczby pierwszej ma się tak, jak jeden do 1024. Gdybyśmy przykładowo chcieli, żeby prawdopodobieństwo to było mniejsze niż jeden do miliona, wówczas trzeba byłoby wykonać jeden po drugim aż 20 tego rodzaju testów. Podobnie, gdyśmy założyli, że prawdopodobieństwo omyłkowego przepuszczenia przez nasze sito liczby złożonej ma być mniejsze niż jeden do miliarda, wtedy liczba wykonywanych jeden po drugim testów pierwszości Solvaya-Strassena musiałby wynieść 30. Jak widać, wykonując odpowiednią liczbę tego rodzaju testów pierwszości prawdopodobieństwo popełniania pomyłki możemy uczynić dowolnie małym. Na przykład po wykonaniu 50 kolejnych testów pierwszości Solvaya-Strassena prawdopodobieństwo przepuszczenia liczby złożonej jako liczby pierwszej będzie już mniejsze niż jeden do biliarda, a zatem w praktyce takie zdarzenie w realnym świecie nie ma w zasadzie prawa już zajść, chociaż nadal zdarzenie takie nie jest bynajmniej zdarzeniem niemożliwym.

Jak już wspomniano, algorytm RSA jest obecnie bardzo popularny, jednak nadal poszukiwane są inne metody zapewniające jeszcze większy poziom kryptograficznego bezpieczeństwa. Jedną z tego rodzaju metod jest tzw. kryptografia krzywych eliptycznych ECC (ang. Eliptic Curve Cryptography). W tym wypadku funkcja jednokierunkowa sprowadza się do wyznaczania wartości logarytmu dyskretnego obliczanego w oparciu o krzywe eliptyczne. Metoda ECC jest techniką szyfrowania asymetrycznego, która jest w stanie zapewnić znacznie wyższy poziom bezpieczeństwa w porównaniu z algorytmem RSA przy tej samej długości klucza. Przykładowo, jeśli w przypadku algorytmu RSA długość klucza wynosi 1024 bity, to taki sam poziom bezpieczeństwa zapewnia technika ECC z kluczem o długości jedynie około 160 bitów.

Jednak obecnie najbardziej perspektywiczna wydaje się dziedzina kryptografii kwantowej, u podstaw której leżą zjawiska zachodzące w obrębie

mikroświata. Świat cząstek elementarnych różni się w sposób istotny od tego, do czego jesteśmy przyzwyczajeni w naszym świecie makroskopowym. Podstawową różnicą jest istnienie w przypadku mikroświata tzw. dualizmu korpuskularno-falowego, który sprowadza się do tego, że każdy obiekt do tego świata należący możemy traktować zarówno jako punktową cząstkę bądź też jako falę, która spełnia tzw. równanie Schroedingera. Istota rozważanego dualizmu korpuskularno-falowego nie została dotychczas w sposób przekonywujący wyjaśniona, a sam fakt, że cząstka elementarna, taka jak na przykład wspomniany elektron, może jednocześnie znajdować się w kilku dowolnie odległych miejscach, wydaje się wręcz przeczyć zdrowemu rozsądkowi. Niestety nasza praktyczna intuicja, pozwalająca nam na co dzień w miarę sprawnie funkcjonować w naszym makroświecie, zawodzi całkowicie, gdy tylko przejdziemy do poziomu mikroświata.

Jak już wspomniano, elektron może jednocześnie znajdować się w dowolnej liczbie miejsc i bynajmniej nie jest tak, że w rzeczywistości jest on tylko i wyłącznie w jednym z nich, a my możemy, w związku z naszą niewiedzą, szacować jedynie wartość prawdopodobieństwa, że on właśnie się w danym miejscu znajduje. Z powyższym zjawiskiem wiąże się tzw. paradoks Einsteina-Podolskiego-Rosena, gdzie informacja o stanie jednej cząstki będącej w stanie splątania kwantowego z inną cząstką rozchodzi się w przestrzeni z nieskończenie wielką prędkością, co stoi w jawnej sprzeczności ze szczególną teorią względności Einsteina, w myśl której informacja nie może być przekazywana z prędkością większą od prędkości światła.

W istocie rozważany elektron jest we wszystkich tych miejscach jednocześnie i dopiero gdy wykonamy pomiar, czyli przeniesiemy zjawisko z poziomu mikroświata do poziomu naszego makroświata, to ostatecznie rozważany elektron ujawnia swą obecność w tylko jednym z tych miejsc. Co ciekawe, nie jest rzeczą do końca jasną, gdzie przebiega ścisła granica pomiędzy mikroświatem, a znanym nam z życia codziennego makroświatem, i dlaczego w obserwowanej na co dzień rzeczywistości makroskopowej nie zachodzą tego rodzaju zjawiska, że przykładowo jakieś duże obiekty istnieją jednocześnie w wielu miejscach.

Z powyższym związany jest słynny paradoks tzw. kota Schroedingera, gdzie foton pada na półprzepuszczalne zwierciadło i z prawdopodobieństwem ½ powoduje w efekcie rozbicie fiolki z cyjankiem, w związku z czym zamknięty w szczelnym pomieszczeniu kot przechodzi do dziwnego stanu będącego superpozycją życia i śmierci i dopiero wykonie pomiaru (zaglądnięcie przez istotę świadomą do wnętrza tego pomieszczania sprawi, że rozważany kot okaże się w końcu ostatecznie żywym bądź całkowicie

martwym). Z kolei pytanie o rolę świadomości w procesie wykonywania pomiarów w rzeczywistości kwantowej doprowadziło do powstania niezwykłej w swej istocie tzw. teorii wielu światów.

Wracając jednak do zagadnień kryptografii, należy powiedzieć, że szyfrowanie kwantowe służy przede wszystkim do przekazywania informacji za pomocą emitowanych kwantów światła (fotonów). W stacji odbiorczej polaryzatory ustawione są pionowo bądź poziomo i w zależności od polaryzacji danego fotonu przechodzi on przez nie bądź nie, co odpowiada wartościom binarnym zera i jedynki. W takim wypadku klucz szyfrujący określa sekwencję użytych polaryzatorów (poziomych bądź pionowych). Dodatkowo należy zaznaczyć, że w zasadzie nie ma możliwości przechwycenia tego rodzaju transmisji bez jej zakłócenia, a przynajmniej jest to wielce nieprawdopodobne, co dodatkowo zabezpiecza transmitowany szyfrogram przed podsłuchem.

BIBLIOGRAFIA

1. Adrian Mencel: *Identyfikacja zagrożeń wynikających z użytkowania systemów informatycznych;* UE Katowice; Academic Review of Business and Economics, 2(1), 79-94. https://doi.org/10.22367/arbe.2022.02.05; ISSN 2720-457X Vol. 2(1), 2022.
2. Raport pełnomocnika rządu ds. cyberbezpieczeństwa: w 2023 r. odnotowano ponad 100-procentowy wzrost cyberataków; https://bydgoszcz.tvp.pl/76947518/raport-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-w-2023-r-odnotowano-ponad-100procentowy--wzrost-cyberatakow.
3. Raport Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ENISA z 2023 roku; https://odoserwis.pl/a/2029/unia-europejska-raport-enisa-z-2023-roku-dotyczacy-krajobrazu-cyberbezpieczenstwa
4. *Global Cybersecurity Outlook* 2023 https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf.
5. *Global geopolitical instability has helped close perception gap between business* https://ciosea.economictimes.indiatimes.com/news/security/global-geopolitical-instability-has-helped-close-the-perception-gap--between-business-and-cyber-leaders-wefs-global-cybersecurity-outlook-2023/97754985.