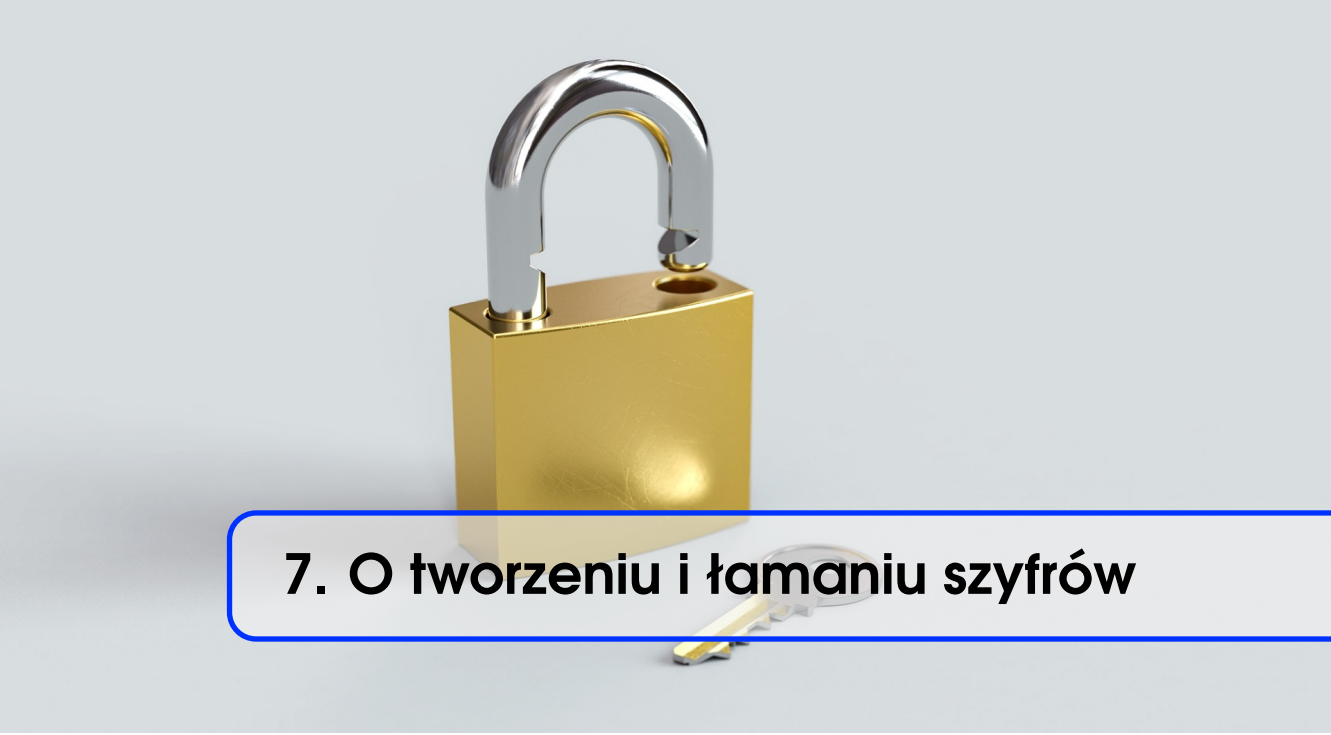


7. O tworzeniu i łamaniu szyfrów

Andrzej Chmielowiec

7.1 Wstęp

Nauka, która zajmuje się tworzeniem i łamaniem szyfrów nazywana jest kryptologią. Składają się na nią dwie podstawowe dziedziny: kryptografia (nauka o tworzeniu szyfrów) i kryptoanaliza (nauka o łamaniu szyfrów). Przez lata rozwoju techniki, zabezpieczania wiadomości ewoluowały i były doskonalone. Jednak dopiero pojawienie się komputerów spowodowało ogromny przełom w tej dziedzinie. Wtedy też okazało się, że rozwijane przez lata, takie działy matematyki jak teoria liczb i algebra abstrakcyjna, mają swoje praktyczne zastosowanie.

Nasze rozważania zacznijmy od przykładu mającego już ponad 2000 lat – *szyfru Cezara*. Zasada jego działania jest z dzisiejszej perspektywy banalnie prosta. Kolejne litery alfabetu łacińskiego $A, B, \ldots, X, Y, Z$ zastępowane są literami odległymi od nich o 3 pozycje, co daje odpowiednio litery $D, E, \ldots, A, B, C$. Nietrudno również wyobrazić sobie proces deszyfrowania, podczas którego następuje odwrotna zamiana. Można zatem powiedzieć, że z matematycznego punktu widzenia szyfrowanie i deszyfrowanie są pewnymi funkcjami, z których druga jest odwrotnością pierwszej. Formalnie dla szyfru Cezara możemy to zapi-

Norway grants

Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).

Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

sać na przykład w następujący sposób:

$$f : \begin{cases} A \mapsto D \\ B \mapsto E \\ C \mapsto F \\ \vdots \\ X \mapsto A \\ Y \mapsto B \\ Z \mapsto C \end{cases} \qquad f^{-1} : \begin{cases} A \mapsto X \\ B \mapsto Y \\ C \mapsto Z \\ \vdots \\ X \mapsto U \\ Y \mapsto V \\ Z \mapsto W \end{cases}$$

Jeśli pójdziemy nieco dalej i zakodujemy każdą literę alfabetu łacińskiego kolejnymi nieujemnymi liczbami całkowitymi ($A \mapsto 0$, $B \mapsto 1$, $\ldots$, $Z \mapsto 25$), to szyfr Cezara przyjmie jeszcze bardziej skondensowaną postać. Mianowicie obie funkcje będziemy mogli zapisać jako

$$\begin{aligned} f(x) &= x + 3 \bmod 26, \\ f^{-1}(y) &= y - 3 \bmod 26. \end{aligned}$$

Przy czym mod26 jest operacją wzięcia reszty z dzielenia przez 26. Zauważmy, że przesunięcie o 3 może być zastąpione przesunięciem o dowolną liczbę pozycji. Wtedy szyfr Cezara uogólnia się do postaci

$$\begin{aligned} f(x,k) &= x + k \bmod 26, \\ f^{-1}(y,k) &= y - k \bmod 26, \end{aligned}$$

gdzie liczbę k nazywamy kluczem. Nietrudno zauważyć, że możliwych kluczy jest 26, przy czym klucz $k = 0$ daje funkcję identycznościową i nie zmienia tekstu jawnego. Klucz taki określamy mianem słabego klucza, gdyż nie pozwala on utajnić wiadomości. Jak do tej pory opisaliśmy konstrukcję szyfru Cezara i jego uogólnienie. Działaliśmy więc w obrębie kryptografii. Teraz spojrzymy na ten szyfr od strony kryptoanalizy, czyli nauki o łamaniu szyfrów. W tym przypadku najprostszą metodą jest tak zwany atak brutalny – to znaczy przeszukanie wszystkich możliwych kluczy kryptograficznych. Atak ten jest możliwy ponieważ liczba wszystkich kluczy jest bardzo mała i wynosi zaledwie 26. Istnieje jednak bardzo prosta modyfikacja szyfru Cezara, która wydatnie zwiększa liczbę możliwych kluczy. Mianowicie jako funkcję f wybieramy dowolną permutację zbioru liter $\{A, B, \ldots, Z\}$. Takich możliwości mamy już $26! \simeq 2^{88}$, co oznacza, że liczba możliwych kluczy jest gigantyczna. Nowoczesny procesor nie byłby w stanie ich przeanalizować nawet gdyby pracował od początku istnienia wszechświata.

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

Tutaj jednak z pomocą przychodzi nam statystyka. Okazuje się bowiem, że w każdym języku częstotliwość występowania poszczególnych liter jest różna. Dzięki temu, przy odpowiedniej liczbie tekstów zaszyfrowanych, możliwe jest znaczne ograniczenie możliwych kluczy. Ten rodzaj kryptoanalizy stosowany był już w średniowieczu. Sprawdzano najpierw, jakie litery pojawiają się w szyfrogramie najczęściej i w to miejsce wstawiano litery najczęściej występujące w danym języku. Na ogół po kilku lub kilkunastu próbach prowadziło to odczytania całej wiadomości i poznaniu przekształcenia szyfrującego.

Szyfry bazujące na koncepcji szyfru Cezara dominowały przez bardzo długi czas. Rewolucję w podejściu do projektowania i łamania szyfrów przyniosła dopiero II Wojna Światowa i niemiecka maszyna szyfrująca Enigma. Była to pierwsza tak zaawansowana koncepcyjnie maszyna szyfrująca. Jej złamanie stało się motorem rozwoju zupełnie nowych metod kryptoanalizy. Ogromny udział mieli w tym polscy matematycy: Marian Rejewski, Henryk Zygalski i Jerzy Różycki. Zastosowali oni teorię permutacji i pewne własności maszyny do ograniczenia przestrzeni przeszukiwanych kluczy. Kolejnego przełomu dokonał Alan Turing, który stworzył tak zwane *bomby kryptologiczne* – urządzenia mechaniczno elektryczne, które wspierały proces łamania szyfru Enigmy. Dały one początek pierwszym komputerom i informatyce.

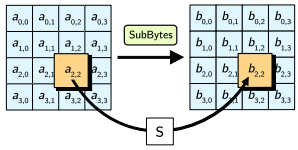
7.2 Współczesne podejście do konstrukcji szyfrów

W roku 1975 nastąpił swego rodzaju przełom w podejściu do projektowania szyfrów. W tym roku opublikowano bowiem standard DES (Data Encryption Standard). Algorytm szyfrowania symetrycznego opracowany przez firmę IBM. Nowością w tym przypadku było opublikowanie kompletnej dokumentacji szyfru. Od początku zatem przyjęto założenie, że bezpieczeństwo szyfrowania zależy jedynie od bezpieczeństwa klucza, a nie utajnienia metody szyfrowania. Zmiana była rewolucyjna o tyle, że przed standardem DES utajniano nie tylko klucze kryptograficzne, ale również sposób szyfrowania. To nowe podejście stało się motorem rozwoju kryptoanalizy szyfrów symetrycznych. Wielu naukowców zajmujących się kryptologią, skupiło swoją uwagę na poszukiwaniu słabości zaproponowanego standardu. Dzięki intensywnym pracom powstały takie techniki, jak kryptoanaliza różnicowa i kryptoanaliza liniowa. Standard ten został wycofany z użytku i zastąpiony szyfrem AES (Advanced Encryption Standard) w roku 2001. Tym razem standard szyfrowania został wyłoniony w ramach otwartego, międzynarodowego konkursu. Algorytm AES stał się, podobnie jak

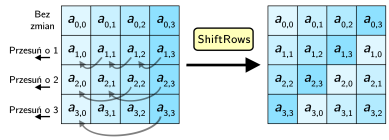
Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

jego poprzednik, kołem zamachowym do badania nowych metod kryptoanalizy. Najbardziej znaczącym efektem prac naukowców była w tym przypadku metoda kryptoanalizy algebraicznej.

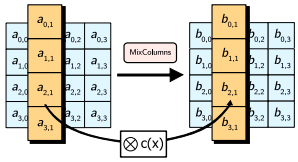
Warto pokazać konstrukcję tego szyfru, gdyż jest ona bardzo estetyczna od strony matematycznej i doskonale pokazuje, w jaki sposób jego autorzy uczynili go odpornym na kryptoanalizę różnicową i liniową. Nie będziemy się tutaj koncentrowali na dokładnym opisie całego szyfru AES, a jedynie na jego pojedynczej rundzie (algorytm realizuje 10, 12 lub 14 rund w zależności od długości klucza).



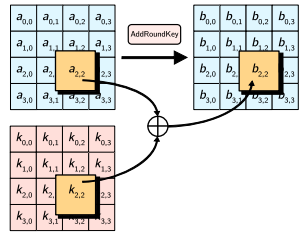
a) Przekształcenia `SubBytes`



b) Przekształcenie `ShiftRows`



c) Przekształcenia `MixColumns`



d) Przekształcenie `AddRoundKey`

Rysunek 7.1: Przekształcenia wchodzące w skład pojedynczej rundy szyfru AES [źródło: domena publiczna]

AES jest szyfrem blokowym szyfrującym porcje danych o długości 128 bitów. Każda taka porcja dzielona jest na 16 bajtów (8-bitowych kawałków). W każdej rundzie te 16 bajtów poddawane jest czterem podstawowym operacjom: `SubBytes`, `ShiftRows`, `MixColumns` i `AddRoundKey`. Działanie poszczególnych operacji zostało zilustrowane na Rysunku 7.1. Z matematycznego punktu widzenia każdy bajt traktowany jest jako element struktury algebraicznej, nazywanej *ciałem*. Jest to taki zbiór elementów, w którym można wykonywać dodawanie, odejmowanie i mnożenie. Dodatkowo istnieje w tym zbiorze 0 i 1, a wszystkie elementy poza zerem mają swoją odwrotność. Każdy bajt `00`, `01`, ..., `FF` traktowany jest jako wielomian

$$\begin{aligned}(B)_{16} &= (b_7b_6b_5b_4b_3b_2b_1b_0)_2 \\ &= b_7X^7 + b_6X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0,\end{aligned}$$

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

a wynik każdej operacji arytmetycznej powstaje przez wykonanie odpowiedniego działania i zredukowanie wyniku do reszty z dzielenia przez wielomian definiujący ciało. W tym przypadku jest to $f(X) = X^8 + X^4 + X^3 + X + 1$. Osoby zainteresowane szczegółami działań arytmetycznych zachęcamy do zapoznania się z tematyką *ciał skończonych* lub *ciał Galois*.

Ćwiczenie 7.1 Aby wykonywać działania w ciele Galois $GF(2^8)$, należy pamiętać o dwóch zasadniczych zasadach:

1. wynik obliczeń zawsze redukujemy do reszty z dzielenia przez wielomian $f(X) = X^8 + X^4 + X^3 + X + 1$,
2. wszystkie liczby parzyste zastępujemy przez 0, a nieparzyste przez 1 – to wynika z tak zwanej *charakterystyki ciała*, która w tym przypadku wynosi 2 (wszystkie współczynniki wielomianów redukowane są do reszty z dzielenia przez 2).

Załóżmy teraz, że mamy przez siebie pomnożyć dwa bajty: `80` i `20`. Bajty te reprezentują dwa wielomiany: $g(X) = X^7$ i $h(X) = X^5$. Iloczyn tych wielomianów to $m(X) = X^{12}$. Teraz konieczne jest wyznaczenie reszty z dzielenia wielomianu m przez f, którą oznaczamy przez $m \bmod f$. W przypadku wielomianów, taka redukcja może być realizowana przez eliminowanie jednomianu o najwyższej potędze. Pamiętając, że liczby parzyste zastępujemy przez 0, a nieparzyste przez 1 możemy dokonać redukcji w następujący sposób:

$$\begin{aligned} m(X) \bmod f(X) &= X^{12} - X^4 f(X) \\ &= X^8 + X^7 + X^5 + X^4 \\ &= X^8 + X^7 + X^5 + X^4 - f(X) \\ &= X^7 + X^5 + X^3 + X + 1. \end{aligned}$$

Możemy zatem zapisać, że `80`·`20` = `AB`. Spróbuj teraz samodzielnie wymnożyć bajty: `80` i `83`. Reprezentują one wielomiany: $g(X) = X^7$ i $h(X) = X^7 + X + 1$. W wyniku tego działania powinieneś otrzymać 1, co oznacza, że jeden z bajtów jest odwrotnością drugiego. ■

Jak dotychczas w szyfrze AES znaleziono jedną słabość. Jest nią przekształcenie `SubBytes`. Z matematycznego punktu widzenia przekształcenie to możemy zapisać jako

$$y = A(x^{-1}) + b,$$

gdzie A jest pewnym odwracalnym przekształceniem liniowym, a b jest ustalonym bajtem. Z algebraicznego punktu widzenia równanie to

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

można przekształcić do postaci

$$xA^{-1}(y-b) = 1.$$

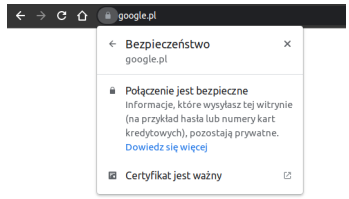
Dzięki temu kryptoanalizę można sprowadzić do rozwiązywania układu równań stopnia drugiego. Wykonując odpowiednie zamiany zmiennych, można ten układ sprowadzić do układu równań liniowych o bardzo dużym rozmiarze. Takie podejście określamy dzisiaj mianem kryptoanalizy algebraicznej. Prace wielu naukowców wskazują, że atak z użyciem opisanej metody może być skuteczniejszy niż przeszukiwanie przestrzeni wszystkich kluczy. Niemniej złożoność tego ataku jest tak duża, że póki co pozostaje on poza zasięgiem obliczeniowym nawet największych superkomputerów.

7.3 Kryptografia z kluczem publicznym – przełom w zabezpieczaniu komunikacji

Podstawowym problemem w stosowaniu kryptograficznej ochrony informacji jest konieczność wcześniejszej wymiany kluczy szyfrujących. Musi się ona odbyć w warunkach całkowitej poufności, a to najczęściej oznacza konieczność albo osobistego spotkania, albo przynajmniej przekazania kluczy przez zaufanego kuriera. Jest to zatem dość kosztowne rozwiązanie jeżeli mówimy o wymianie informacji z kimś, kto znajduje się na drugim końcu Świata. Rozwiązanie tego problemu przyniosła druga połowa lat 70-tych XX wieku. W roku 1976 Witfield Diffie oraz Martin Hellman zaproponowali pierwszy protokół, pozwalający na ustalenie wspólnego sekretu (klucza szyfrującego) przy użyciu publicznego kanału komunikacyjnego. Rok później Ron Rivest, Adi Shamir i Leonard Adleman zaproponowali algorytm szyfrowania asymetrycznego oraz podpisu cyfrowego. Obie te metody zrewolucjonizowały podejście do zabezpieczania informacji i dały podwaliny do bezpiecznej komunikacji elektronicznej.

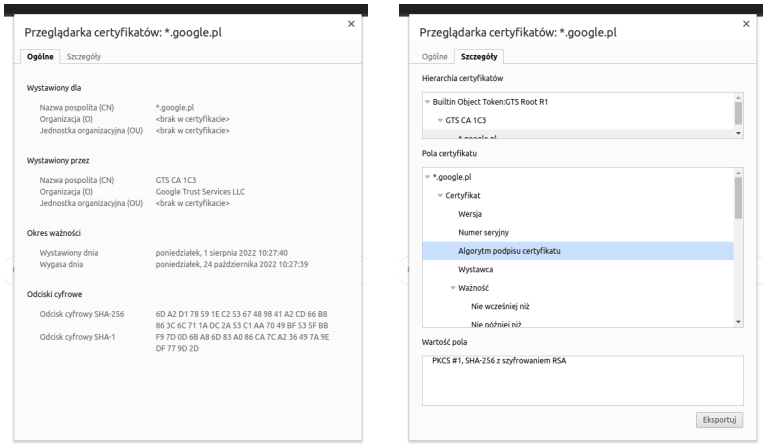
Dzisiaj niemal każda witryna posiada swój cyfrowy certyfikat i umożliwia nawiązanie z nią bezpiecznej, szyfrowanej komunikacji. Na Rysunku 7.2 przedstawiono komunikat przeglądarki Chrome, która informuje o zabezpieczonej transmisji z witryną google.pl.

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.



Rysunek 7.2: Informacja przeglądarki na temat zabezpieczenia połączenia z witryną (połączenie szyfrowane protokołem HTTPS)

Szczegóły cyfrowego certyfikatu przedstawiono na Rysunku 7.3. Certyfikat jest dokumentem podpisanym cyfrowo, który zawiera informacje dotyczące właściciela, klucza publicznego, użytych algorytmów oraz sposobu użycia klucza. Dzięki tym informacjom przeglądarka może nawiązać bezpieczne połączenie ze stroną internetową. Taka zaszyfrowana transmisja jest dzisiaj podstawą wszelkich usług bankowych i sklepów internetowych.



Rysunek 7.3: Informacja przeglądarki na temat certyfikatu wykorzystane do zabezpieczenie komunikacji ze stroną internetową (w szczegółach informacja na temat zastosowania algorytmu RSA do podpisania certyfikatu)

Pozostawmy jednak stronę techniczną i zobaczmy, jaka matematyka kryje się za protokołem Diffiego-Hellmana i algorytmem RSA. Podstawę obu systemów stanowi arytmetyka resztowa. Mieliśmy już z nią do czynienia przy okazji szyfru Cezara. Określiliśmy bowiem prze-

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

kształcenie szyfrujące jako $f(x) = x + 3 \bmod 26$. Zatem interesowały nas tak naprawdę reszty z dzielenia przez 26. W przypadku protokołu Diffiego-Hellmana (DH) wykorzystujemy podobny mechanizm. Zakładamy bowiem, że znana jest pewna duża liczba pierwsza p oraz pewna liczba g zwana generatorem o tej własności, że zbiór

$$\langle g \rangle = \{g^1 \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p\}$$

zawiera wszystkie reszty z dzielenia od 1 do $p-1$. Aby protokół DH był odporny na różnego rodzaju ataki, poszukuje się liczb pierwszych postaci $p = 2q+1$, gdzie q również jest liczbą pierwszą. Wbrew pozorom, znalezienie liczby pierwszej o takich własnościach nie jest wcale trudne. Wynika to przede wszystkim z faktu, że gęstość liczb pierwszych, w zbiorze liczb naturalnych, jest relatywnie duża. Można bowiem wykazać, że liczb pierwszych mniejszych od n jest mniej więcej $\frac{n}{\ln n}$. Oznacza to, że średnio, co $(\ln n)$-ta liczba jest pierwsza. Do weryfikacji, czy liczba naturalna jest liczbą pierwszą stosowane są różnego rodzaju testy. Jednym z najpopularniejszych jest test Rabina-Millera. Jest to test probabilistyczny o bardzo dużej szybkości.

Ćwiczenie 7.2 Rozważmy liczbę pierwszą $p = 2q+1 = 11 = 2 \cdot 5 + 1$. Można wykazać, że dla liczb pierwszych postaci $2q+1$ na to, aby liczba g była generatorem potrzeba i wystarcza spełnienie dwóch następujących zależności:

1. $g^2 \bmod p \neq 1$,
2. $g^q \bmod p \neq 1$.

Dzięki powyższemu warunkowi możemy zatem stwierdzić, że liczba 2 jest generatorem dla liczby 11, gdyż $2^2 \bmod 11 = 4 \neq 1$ oraz $2^5 \bmod 11 = 10 \neq 1$. Natomiast liczba 10 nie jest generatorem, gdyż $10^2 \bmod 11 = 1$. Wyznacz wartości wyrażeń $2^k \bmod 11$ dla liczb $k \in \{1, 2, \ldots, 10\}$ i sprawdź, że żadna wartość nie została powtórzona. Znajdź generator dla liczby pierwszej $p = 23 = 2 \cdot 11 + 1$.

■

Mając do dyspozycji liczbę pierwszą p oraz wspomniany generator g możemy zrealizować protokół opracowany przez Diffiego i Hellmana. Zakładamy przy tym, że wartości p i g są publicznie znane wszystkim stronom. Przyjmijmy, że Alicja i Bob chcą w bezpieczny sposób komunikować się ze sobą na przykład za pomocą szyfru AES. Aby to zrobić muszą posiadać klucz, który będzie znany tylko im. Zadaniem protokołu DH jest właśnie ustalenie wspólnego sekretu znanego tylko Alicji i Bobowi.

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

Alicja	Internet	Bob
Wylosowanie klucza $a \in \{1, 2, \ldots, p-1\}$		Wylosowanie klucza $b \in \{1, 2, \ldots, p-1\}$
Wyznaczenie $h_a = g^a \bmod p$		Wyznaczenie $h_b = g^b \bmod p$
	$h_a \rightarrow$ $\leftarrow h_b$	
Wyznaczenie $k = (h_b)^a \bmod p$ $= (g^b)^a \bmod p$ $= g^{ab} \bmod p$		Wyznaczenie $k = (h_a)^b \bmod p$ $= (g^a)^b \bmod p$ $= g^{ab} \bmod p$

Jak widzimy, Alicja i Bob są w stanie wyznaczyć identyczną wartość k, przy czym w kanale transmisyjnym pojawiają się jedynie wartości h_a oraz h_b. Całe bezpieczeństwo tego protokołu oparte jest na założeniu, że wyznaczenie sekretu $g^{ab} \bmod p$ jest obliczeniowo bardzo trudne, jeżeli znane są jedynie $p, g, h_a = g^a \bmod p$ i $h_b = g^b \bmod p$. Zatrzymajmy się teraz przez chwilę nad stwierdzeniem *obliczeniowo bardzo trudne*. Jest ono dzisiaj podstawą wszelkich zabezpieczeń teleinformatycznych. To znaczy wyszukujemy problem, którego rozwiązanie z obliczeniowego punktu widzenia wymaga niewyobrażalnych zasobów i próbujemy na jego bazie stworzyć algorytm szyfrowania, podpisu cyfrowego lub wymiany kluczy. Należy przy tym pamiętać, że naukowcy cały czas poszukują nowych, lepszych metod rozwiązywania wielu problemów obliczeniowych. Może się zatem zdarzyć, że konieczne stanie się wydłużenie kluczy bądź nawet zmiana systemu zabezpieczeń. Na przykład na początku tego stulecia dla protokołu DH powszechnie używano liczb pierwszych, które mają 1024 bity. Dzisiaj dopuszcza się długości nie mniejsze niż 3072 bity. Natomiast dla nowych aplikacji rekomendowane jest zastąpienie arytmetyki liczbowej przez arytmetykę na punktach krzywej eliptycznej. Z uwagą należy się również przyglądać rozwojowi komputerów kwantowych. Dla takich komputerów problem stanowiący podstawę bezpieczeństwa protokołu DH jest bowiem obliczeniowo łatwy.

Przejdźmy teraz do algorytmu RSA. Jest to o tyle fenomenalne rozwiązanie, że daje możliwość zarówno realizacji szyfrowania z kluczem publicznym, jak i wykonywania podpisu cyfrowego. Algorytm ten na długie dekady zagościł w niemal wszystkich implementacjach służących do ochrony transmisji danych. Podstawą jego bezpieczeństwa jest problem rozkładu liczb na czynniki pierwsze. Aby zrealizować algorytm

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

RSA, należy wygenerować dwie liczby pierwsze p oraz q, a następnie wyznaczyć ich iloczyn $n = pq$. Dodatkowo generujemy parę kluczy kryptograficznych: klucz publiczny e oraz klucz prywatny d o tej własności, że

$$ed \bmod (p-1)(q-1) = 1.$$

Klucz publiczny e wraz z liczbą n udostępniamy wszystkim zainteresowanym nawiązaniem z nami bezpiecznego połączenia. Natomiast klucz prywatny d oraz liczby pierwsze p i q przechowujemy w bezpiecznym miejscu. Załóżmy, że ktoś chce do nas zaszyfrować pewną wiadomość m. Wtedy wyznacza szyfrogram c w następujący sposób

$$c = m^e \bmod n.$$

Aby odszyfrować przesłaną wiadomość c, konieczne jest posiadanie klucza prywatnego d

$$t = c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n.$$

Tylko dlaczego t powinno dawać wartość zaszyfrowanej wiadomości m? Okazuje się, że odpowiedzi na to pytanie udzielił już kilka wieków wcześniej Leonard Euler, który sformułował następujące twierdzenie

Twierdzenie 7.1 Jeżeli największy wspólny dzielnik liczb a i n wynosi 1, to zachodzi następująca zależność

$$a^{\varphi(n)} \bmod n = 1,$$

gdzie $\varphi(n)$ jest liczbą liczb naturalnych względnie pierwszych z n i mniejszych od n. W szczególności, jeżeli $n = pq$, to $\varphi(n) = (p-1)(q-1)$.

Aby wyjaśnić, dlaczego powyższe twierdzenie pozwala na skuteczne deszyfrowanie wiadomości, musimy powrócić do warunku narzuconego na klucze e i d. Przypomnijmy, że spełniają one zależność $ed \bmod (p-1)(q-1) = 1$. Z definicji dzielenia z resztą oznacza to, że istnieje pewna całkowita i nieujemna liczba s, która spełnia równanie $ed = s(p-1)(q-1) + 1$. Zatem możemy zapisać

$$\begin{aligned} m^{ed} \bmod n &= m^{s(p-1)(q-1)+1} \bmod n \\ &= \left(m^{(p-1)(q-1)}\right)^s \cdot m \bmod n. \end{aligned}$$

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

Twierdzenie Eulera mówi nam jednak, że jeżeli m i n są względnie pierwsze, to $m^{(p-1)(q-1)} \bmod n = 1$. Otrzymujemy zatem

$$t = m^{ed} \bmod n = (1)^s \cdot m \bmod n = m.$$

Co jednak w przypadku, gdy wiadomość m nie jest względnie pierwsza z n. Można wykazać, że również w takich przypadkach proces deszyfrowania daje poprawną wartość. Z taką wiadomością jest jednak poważniejszy problem. Znalezienie takiej niezerowej wiadomości oznacza bowiem możliwość wyznaczenia czynników p i q. W konsekwencji posiadacz takiego m może również wyznaczyć klucz prywatny d i złamać kryptosystem. Pamiętajmy jednak, że minimalna długość kiedykolwiek stosowanych kluczy RSA wynosi 1024 bity. W praktyce oznacza to tyle, że wylosowanie takiej wiadomości jest tak samo prawdopodobne jak wygrana w Lotto 16 razy z rzędu.

Algorytm RSA posiada sporo luk, które można wyeliminować przez narzucenie odpowiednich warunków na czynniki p i q. Dodatkowo wprowadza się również specjalne formatowanie wiadomości, aby zmniejszyć ryzyko nieuprawnionego jej odczytania. Za pomocą RSA można również realizować podpis cyfrowy. Przebieg obliczeń jest podobny, tylko w pierwszej kolejności wykorzystywany jest wykładnik prywatny d. Za jego pomocą tworzony jest podpis

$$h = m^d \bmod n.$$

Następnie autor udostępnia parę (m, h) oraz swój klucz publiczny (e, n). Dzięki temu każdy może zweryfikować, czy podpis pod wiadomością jest autentyczny. Jeżeli bowiem wartość

$$t = h^e \bmod n$$

jest tożsama z m, to uznajemy podpis za poprawny i złożony przez posiadacza klucza prywatnego d. W przeciwnym razie uznajemy podpis za fałszywy.

7.4 Podsumowanie

Przedstawione w tym rozdziale tematy, związane z szyfrowaniem i podpisami cyfrowymi, stanowią jedynie wstęp do obszernej dziedziny, jaką jest kryptologia. Celem tego rozdziału było pokazanie, w jaki sposób nowoczesne metody bezpieczeństwa teleinformatycznego bazują na matematyce i jak istotna jest ona w zapewnieniu poufności i niezaprzeczalności transmisji cyfrowej. Czytelników zainteresowanych tą tematyką odsyłamy do obszernej literatury dotyczącej tematu kryptograficznej ochrony informacji.

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.