Szyfry z publicznym kluczem

Wojciech GUZICKI

W poprzednim artykule (*Delta* 1/1997) poznaliśmy przykłady tzw. szyfrów klasycznych. Popatrzmy jeszcze raz, na czym polega szyfrowanie za pomocą takich szyfrów. Przede wszystkim dzielimy tekst, który chcemy zaszyfrować, na tzw. jednostki tekstu. W naszych przykładach były to pojedyncze litery, ale można też używać par, trójek, czwórek liter itd. Każdą jednostkę tekstu zastępowaliśmy inną jednostką tekstu i z nich składaliśmy tekst zaszyfrowany. Na przykład, w klasycznym szyfrze Cezara jednostkę tekstu A zastępowaliśmy jednostką tekstu D, a jednostkę K – jednostką N.

Spróbujmy teraz sformalizować pojęcie systemu kryptograficznego. Niech $\mathcal{P}$ będzie zbiorem wszystkich jednostek tekstu używanych w tekstach jawnych, a $\mathcal{C}$ zbiorem wszystkich jednostek tekstu używanych w tekstach zaszyfrowanych (te dwa zbiory mogą być równe, jak w dotychczasowych przykładach, a mogą też być różne). Niech $\mathcal{E}$ będzie zbiorem kluczy szyfrowania i $\mathcal{D}$ zbiorem kluczy rozszyfrowywania. Szyfrowanie polega wtedy na obliczaniu wartości pewnej funkcji $f : \mathcal{P} \times \mathcal{E} \to \mathcal{C}$, a rozszyfrowywanie – na obliczaniu wartości funkcji w pewnym sensie odwrotnej $g : \mathcal{C} \times \mathcal{D} \to \mathcal{P}$. Jeżeli mamy dany pewien klucz szyfrowania $e \in \mathcal{E}$ i odpowiadający mu klucz rozszyfrowywania $d \in \mathcal{D}$, to jednostkę tekstu jawnego P szyfrujemy jako $f(P, e)$, a jednostkę tekstu zaszyfrowanego C rozszyfrowujemy jako $g(C, d)$. Oczywiście, dla każdej jednostki tekstu P musi zachodzić równość

$$g(f(P, e), d) = P\,.$$

Klasyczne systemy szyfrowania to takie systemy, w których klucze e i d albo są identyczne, albo jeden z nich można łatwo otrzymać z drugiego. Co to znaczy, że jeden z tych kluczy można łatwo otrzymać z drugiego? Otóż znaczy to, że istnieje szybko działający algorytm, za pomocą którego możemy wyznaczyć klucz d, jeśli znamy klucz e. Na przykład, jeśli kluczem szyfrowania była pewna permutacja liter alfabetu łacińskiego, to klucz rozszyfrowywania wyznaczamy szybko, znajdując permutację odwrotną. Szyfry z publicznym kluczem to takie szyfry, dla których nie znamy żadnego szybko działającego algorytmu, za pomocą którego moglibyśmy znaleźć klucz rozszyfrowywania, jeśli znamy klucz szyfrowania.

Zobaczymy teraz przykład takiego szyfru. Ten system kryptograficzny, opracowany w 1978 roku przez trzech matematyków (R.L. Rivesta, A. Shamira i L.M. Adlemana) i nazywany w skrócie (od nazwisk autorów) szyfrem RSA, jest dziś jednym z najbardziej popularnych szyfrów z publicznym kluczem. Główny pomysł tego szyfru polega na tym, że wybieramy dużą liczbę złożoną n, której rozkład na czynniki pierwsze znamy; dużą na tyle, by nikt inny nie umiał rozłożyć jej na czynniki. Okazuje się bowiem, że dotychczas nie znamy żadnego szybko działającego algorytmu, za pomocą którego moglibyśmy rozkładać na czynniki liczby mające nieco ponad 100 cyfr (w systemie dziesiętnym). Klucz szyfrowania możemy dobrać prawie dowolnie. Jednak aby z tego klucza szyfrowania otrzymać klucz rozszyfrowywania, potrzebna jest znajomość czynników pierwszych liczby n. My te czynniki znamy i dlatego umiemy szybko ten klucz znaleźć. Nikt inny tych czynników nie zna, więc nie potrafi znaleźć klucza rozszyfrowywania. Klucz szyfrowania może więc być podany do wiadomości wszystkim, a tylko my będziemy znali klucz rozszyfrowywania. Przyjrzyjmy się teraz temu systemowi dokładniej.

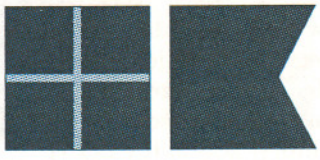
Jednostki tekstu kodujemy za pomocą liczb naturalnych. Każdej literze przypiszemy ciąg dwóch cyfr: A = 01, B = 02, ..., Z = 26. Przyjmijmy na początek, że jednostkami tekstu będą pary liter. Parę WG kodujemy za pomocą czterech cyfr: 2307. Parę AB kodujemy za pomocą cyfr 0102, czyli po prostu za pomocą liczby 102. W ten sposób każda jednostka tekstu zostanie zakodowana za pomocą liczby trzycyfrowej lub czterocyfrowej. Następnie wybieramy dwie liczby pierwsze p i q i mnożymy je: $n = p \cdot q$. Liczby p i q dobieramy w taki

Oto przykład, w którym jednostkami tekstu są pary liter. Nie rozróżniamy liter I oraz J; zawsze piszemy I. Litery takiego uproszczonego alfabetu zapisujemy w dowolnej kolejności w tabelce o pięciu wierszach i pięciu kolumnach:

R V M H Y
F A S U Q
P Z D N K
T G L B C
E I O W X

Pary liter szyfrujemy następująco: jeśli obie znajdują się w jednym wierszu, jak np. FU, to zamiast każdej bierzemy następną literę z tego samego wiersza. Zamiast FU weźmiemy więc AQ. Oczywiście, zamiast ostatniej litery bierzemy pierwszą. Jeśli obie znajdują się w tej samej kolumnie, to bierzemy następne litery z tej samej kolumny: zamiast DO – LM. Wreszcie, jeśli obie litery znajdują się w różnych wierszach i różnych kolumnach, np. FB, to zamiast pierwszej litery F bierzemy literę z tego wiersza co F i z tej kolumny co B, a więc U, a zamiast drugiej litery B bierzemy literę z tego wiersza co B i tej kolumny co F, czyli T. Parę FB szyfrujemy więc jako UT. Ten system szyfrowania nazywany jest szyfrem Playfaira.

Korzystając z tablic częstości występowania par liter również taki szyfr można złamać metodami statystycznymi.



RB – Wlokę moją kotwicę.

Rozwiązanie zadania F 448. Na rakietę spadającą swobodnie w tunelu działa siła

$$F = \frac{mgr}{R}$$

(m jest masą rakiety, a r odległością od środka Ziemi), a jej energia potencjalna wynosi

$$E_p = \frac{mgr^2}{2R}.$$

Korzystając z zasady zachowania energii

$$\frac{1}{2}mgR = \frac{1}{2}mv_0^2$$

wyznaczamy prędkość rakiety w środku Ziemi. Otrzymujemy

$$v_0 = \sqrt{gR}$$

(jest ona równa pierwszej prędkości kosmicznej).

Niech Δv będzie przyrostem prędkości, jakiego musi doznać rakieta mijając środek Ziemi, aby na jej powierzchni uzyskała wartość v_{II}. Z zasady zachowania energii

$$\frac{1}{2}m(v_0 + \Delta v)^2 = \frac{1}{2}mv_{II}^2 + \frac{1}{2}mgR$$

otrzymujemy

$$\Delta v = \frac{\sqrt{3}-1}{\sqrt{2}}v_{II} \approx 5{,}8 \text{ km/s}.$$

Żeby zrozumieć ten wynik, zauważmy, że dla rakiety startującej z powierzchni Ziemi, zgodnie z zasadą zachowania pędu, część energii wytworzonej w silniku zostanie zużyta na nadanie energii kinetycznej gazom wypływającym z dysz silnika.

Jeśli jednak rakieta ma pewną prędkość, to energia przekazywana gazom jest mniejsza. Na przykład, gdyby prędkość wypływu gazów względem rakiety była równa prędkości rakiety względem Ziemi, to prędkość gazów względem Ziemi byłaby równa zeru, czyli cała energia wytworzona w silniku zostałaby przekazana rakiecie. Zadanie to pokazuje, że pole grawitacyjne można wykorzystać w nawigacji międzyplanetarnej, co rzeczywiście czyni się wykorzystując pole grawitacyjne ciężkich planet (Jowisz, Saturn) w misjach sond takich, jak Voyager.

sposób, by wszystkie jednostki tekstu były kodowane liczbami mniejszymi niż n. Na przykład, możemy wziąć $p = 109$ i $q = 137$. Wtedy liczba $n = 14933$ jest większa od największego możliwego kodu pary liter: dla pary ZZ tym kodem jest liczba 2626.

Liczby p i q trzymamy w tajemnicy, natomiast ujawniamy wszystkim liczbę n. Oczywiście, jeśli liczby p i q są małe, to liczbę n bez trudu możemy rozłożyć na czynniki. Nawet korzystając tylko z niewielkiego kalkulatora, zrobiłby to Czytelnik w podanym wyżej przypadku nie dłużej niż w parę minut. Jednak w poważnych zastosowaniach wybieramy znacznie większe liczby pierwsze, np. stucyfrowe. Rozłożenie liczby n na czynniki jest wtedy praktycznie niemożliwe.

Teraz znajdujemy klucze: szyfrowania i rozszyfrowywania. W tym celu obliczamy najpierw wartość tzw. funkcji Eulera $\varphi(n)$ dla liczby n. Liczba $\varphi(n)$ jest liczbą tych liczb dodatnich i nie większych od n, które są względnie pierwsze z liczbą n, tzn. nie mają wspólnych z n dzielników większych od 1. Nietrudno stwierdzić, że jeśli liczba n jest iloczynem dwóch liczb pierwszych p i q, to $\varphi(n) = (p-1)\cdot(q-1)$. Ponieważ znamy liczby p i q, to możemy łatwo obliczyć $\varphi(n)$. Zauważmy jednak, że nikt inny nie będzie umiał tego zrobić. Nie znamy bowiem dotychczas właściwie żadnej innej metody obliczania $\varphi(n)$.

Następnie wybieramy jakąkolwiek liczbę e względnie pierwszą z $\varphi(n)$. O tym, czy dwie liczby są względnie pierwsze, możemy przekonać się łatwo (i szybko) za pomocą algorytmu Euklidesa. W naszym przykładzie mamy $\varphi(n) = 14688$ i jako liczbę e możemy wziąć np. 13. Łatwo sprawdzić, że 13 nie jest dzielnikiem liczby 14688. Ponieważ 13 to liczba pierwsza, więc jest też względnie pierwsza z liczbą 14688. Liczba e będzie wraz z liczbą n kluczem szyfrowania. Wreszcie musimy znaleźć odpowiadający temu kluczowi klucz rozszyfrowywania. Korzystamy w tym celu z następującego prostego twierdzenia:

Twierdzenie. Jeśli liczby a i m są względnie pierwsze, to istnieje taka liczba b, że $ab \equiv 1 \pmod{m}$.

Uwaga: Przypominamy, że $x \equiv y \pmod{m}$ wtedy i tylko wtedy, gdy m dzieli $x - y$.

Szkic dowodu. Korzystając z algorytmu Euklidesa znajdujemy takie liczby b i c, że $ab + mc = 1$. Wtedy $ab \equiv 1 \pmod{m}$.

Kluczem rozszyfrowywania będzie liczba d, dla której zachodzi kongruencja $ed \equiv 1 \pmod{\varphi(n)}$. Zauważmy, że jeśli znamy klucz e i chcemy poznać klucz d, to najpierw powinniśmy obliczyć $\varphi(n)$, a dopiero potem zastosować algorytm Euklidesa. Nie znamy przy tym właściwie żadnej innej metody znajdowania klucza d. Tak więc, jeśli będziemy trzymać w tajemnicy obie liczby pierwsze p i q, to nikt inny nie będzie mógł obliczyć $\varphi(n)$ i tym samym nie będzie mógł znaleźć klucza d.

Mamy już oba klucze e i d. Trzeba tylko pokazać, w jaki sposób ich używamy. Przypuśćmy więc, że jakąś jednostkę tekstu zakodowaliśmy za pomocą pewnej liczby a mniejszej niż n. Definiujemy

$$f(P,e) = (P^e \bmod n) \qquad \text{oraz} \qquad g(C,d) = (C^d \bmod n).$$

Zarówno dziedziną, jak i przeciwdziedziną obu tych funkcji jest zbiór liczb naturalnych mniejszych od n. Każda jednostka tekstu jawnego ma kod należący do tego zbioru, więc może być zaszyfrowana. Po zaszyfrowaniu otrzymamy liczbę mniejszą od n, możemy więc ją rozszyfrować za pomocą funkcji g. Czy otrzymamy z powrotem tę samą jednostkę tekstu jawnego? Okazuje się, że tak i wynika to dość łatwo z następującego twierdzenia Eulera:

Twierdzenie. Jeśli liczby a i m są względnie pierwsze, to $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Nietrudny dowód tego twierdzenia można znaleźć w każdym podręczniku elementarnej teorii liczb. Niech teraz P będzie kodem dowolnej jednostki tekstu. Załóżmy przy tym, że liczby P i n są względnie pierwsze.
To założenie nie ogranicza w istotny sposób zakresu stosowalności szyfru RSA. Prawdopodobieństwo znalezienia jednostki tekstu, której kod byłby liczbą podzielną przez p lub przez q, jest tak małe, że można się tym nie przejmować.

W naszym przykładzie kluczem szyfrowania była liczba 13. Zastosowanie algorytmu Euklidesa daje nam klucz rozszyfrowywania: $d = 7909$. Jednostkę tekstu o kodzie 2307 szyfrujemy podnosząc liczbę 2307 do potęgi 3 modulo 14933. Nietrudno przekonać się za pomocą krótkiego programu komputerowego, że otrzymamy wynik 11596. Aby go rozszyfrować, musimy podnieść liczbę 11596 do potęgi 7909 modulo 14933. Za pomocą tego samego programu komputerowego przekonamy się, że ta potęga jest równa 2307.

Rozwiązanie zadania F 447. Niech x_1 i x_2 oznaczają położenia przednich zderzaków każdego z samochodów, natomiast v_1 i v_2 prędkości obu samochodów. Ruch pierwszego samochodu opisują równania

$$v_1 = at\,,$$
$$x_1 = \frac{1}{2}at^2\,.$$

Drugi samochód startuje z położenia $x_2 = -l$. Jego prędkość jest związana z położeniami obu samochodów zależnością

$$v_2 = \frac{\mathrm{d}x_2}{\mathrm{d}t} = k(x_1 - x_2 - l)\,,$$

gdzie $k = \text{const}$. Niech $f = (x_2 + l)\mathrm{e}^{kt}$. Funkcja ta spełnia równanie

$$\frac{\mathrm{d}f}{\mathrm{d}t} = \frac{1}{2}kat^2\mathrm{e}^{kt}\,.$$

Całkując je i korzystając z warunków początkowych otrzymujemy

$$x_2 = \frac{1}{2}at^2 - \frac{at}{k} + \frac{a}{k^2}\left(1 - \mathrm{e}^{-kt}\right) - l\,.$$

Z tego, że $ed \equiv 1 \pmod{\varphi(n)}$, wynika, iż istnieje taka liczba naturalna k, że $ed = k \cdot \varphi(n) + 1$. Mamy wtedy na mocy twierdzenia Eulera

$$g(f(P,e),d) \equiv f(P,e)^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{k\varphi(n)+1} \equiv$$
$$\equiv \left(P^{\varphi(n)}\right)^k \cdot P \equiv 1 \cdot P \equiv P \pmod{n}\,.$$

Zatem rzeczywiście operacja rozszyfrowywania jest operacją odwrotną do szyfrowania.

A oto przykład poważniejszy. Weźmy znów zdanie `ALEA IACTA EST` i potraktujmy je jako jedną jednostkę tekstu. Kodem tego zdania, po opuszczeniu przerw i zera na początku, będzie liczba $P = 112050109010320010519 20$. Wybieramy w tajemnicy dwie liczby pierwsze p i q i podajemy ich iloczyn: $n = 24543265623376954208 3107$. Kluczem szyfrowania będzie znów liczba 13. Tym razem podniesienie liczby P do potęgi 13 jest trochę bardziej pracochłonne, ale znów krótki program komputerowy poradzi sobie z tym zadaniem w mgnieniu oka. Oczywiście, ten program musi korzystać z jakichś procedur umożliwiających wykonywanie podstawowych działań arytmetycznych na bardzo dużych liczbach. Problem pojawi się chwilę później. Po zaszyfrowaniu otrzymamy liczbę $C = 29070537299022241578466$. Aby rozszyfrować nasze zdanie, będziemy musieli podnieść liczbę C do potęgi d. Tym razem jednak d jest bardzo dużą liczbą: ma ona 23 cyfry! Jak więc podnieść liczbę C do tak dużej potęgi? Ile czasu będzie to trwało?

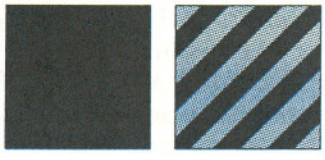
Zastanówmy się przez chwilę, ile mnożeń trzeba wykonać, by podnieść daną liczbę a do potęgi k. Wydaje się w pierwszej chwili, że musimy wykonać $k-1$ mnożeń: najpierw obliczyć $a^2 = a \cdot a$, potem $a^3 = a^2 \cdot a$, potem $a^4 = a^3 \cdot a$ itd. A jednak można to zrobić znacznie szybciej. Popatrzmy na przykład. Aby obliczyć a^{16}, wystarczą cztery mnożenia. Obliczamy kolejno: $a^2 = a \cdot a$, $a^4 = a^2 \cdot a^2$, $a^8 = a^4 \cdot a^4$ i wreszcie $a^{16} = a^8 \cdot a^8$. W podobny sposób, podwajając za każdym razem wykładnik, możemy bardzo szybko obliczyć potęgę a^k modulo n dla wykładnika k będącego potęgą liczby 2. Jeśli teraz pomnożymy odpowiednie takie potęgi (oczywiście, nadal modulo n), to otrzymamy potęgę o zadanym z góry wykładniku k. Wynika to stąd, że każda liczba k jest sumą pewnych potęg liczby 2. Ten algorytm pozwala na wykonanie w krótkim czasie dowolnego potęgowania modulo n, a więc umożliwia dość szybkie szyfrowanie i rozszyfrowywanie.

Aby sobie lepiej uzmysłowić, co to znaczy, niech Czytelnik spróbuje znaleźć klucz rozszyfrowywania w powyższym przykładzie. Liczba n jest iloczynem dwóch dwunastocyfrowych liczb pierwszych p i q. Może komuś uda się rozłożyć liczbę n na czynniki pierwsze i znaleźć następnie klucz d! Za miesiąc podam te liczby p i q.

Zauważmy, że nie tylko sam algorytm szyfrowania jest znany wszystkim. Znany jest też klucz szyfrowania. A mimo to klucz rozszyfrowywania jest znany tylko „właścicielowi" szyfru.

Jakie jest znaczenie takich szyfrów z publicznym kluczem? Przypuśćmy, że chcemy wysłać do kogoś pocztą elektroniczną zaszyfrowaną wiadomość. W tym celu musielibyśmy najpierw spotkać się z tą osobą, wymienić klucze szyfrowania i rozszyfrowywania, a potem dopiero używać ich do korespondencji. To byłoby bardzo niewygodne. Bardzo często łączymy się z osobami znajdującymi się na innych kontynentach, lub z osobami czy instytucjami (np. z bankami), z którymi spotykamy się bardzo rzadko. Otóż systemy kryptograficzne z publicznym kluczem umożliwiają następującą wymianę korespondencji. Najpierw piszemy do kogoś, że mamy dla niego poufną wiadomość. Umawiamy się, że do zaszyfrowania użyjemy szyfru RSA. Następnie prosimy tego kogoś o przysłanie nam (w jawny sposób!) jego klucza szyfrowania. Oczywiście, swoje liczby p, q, $\varphi(n)$ i d trzyma on w tajemnicy. Teraz możemy zaszyfrować wiadomość i przesłać mu ją powszechnie dostępnym kanałem informacyjnym. Nikt jednak, nawet jeśli podpatrzył całą naszą wcześniejszą korespondencję, nie będzie umiał rozszyfrować tekstu raz zaszyfrowanego. Rozszyfrować potrafi tylko adresat: właściciel liczb pierwszych p i q i tym samym jedyny właściciel klucza d.

Do wyjaśnienia pozostaje właściwie tylko jedna kwestia. Jak znaleźć te duże liczby pierwsze p i q i jak przekonać się, że są one naprawdę pierwsze? Wspomniałem wyżej, że nie umiemy rozkładać dużych liczb na czynniki i ten właśnie fakt decydował o bezpieczeństwie szyfru RSA. Czy potrafimy zatem przekonać się, że duża liczba jest pierwsza, w inny sposób, niż próbując rozłożyć ją na czynniki? Tym problemem zajmiemy się w następnym artykule.



EY – Jestem pewien swojej pozycji.