Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 242 · 2015

Ekonomia 3

Andrzej Wilkowski

Uniwersytet Ekonomiczny we Wrocławiu
Wydział Zarządzania, Informatyki i Finansów
Katedra Matematyki i Cybernetyki
andrzejm.wilkowski@gmail.com

O BEZPIECZEŃSTWIE INTERNETOWYM

Streszczenie: W pracy omówiono kryptosystemy oparte na krzywych eliptycznych oraz metodę szyfrowania dynamicznego ZT-UNITAKOD. Są to nowe narzędzia zwiększające bezpieczeństwo internetowe. Przedstawiono także sposoby przeciwdziałania phishingowi.

Słowa kluczowe: kryptosystem z kluczem publicznym, szyfrowanie dynamiczne, krzywa eliptyczna, phishing.

Wprowadzenie

Praca ma charakter przeglądowy. Jej celem jest przedstawienie nowych metod pozwalających zwiększyć bezpieczeństwo teleinformatyczne. W pkt. 1 przedstawiono analizę incydentów naruszających bezpieczeństwo teleinformatyczne w roku 2012 w Polsce, zawarte w raporcie zespołu CERT. Dalej omówiono kryptosystemy z kluczem publicznym i długości kluczy kryptograficznych z nimi związanych, uważanych obecnie za bezpieczne. Punkt 3 poświęcony jest wykorzystaniu teorii krzywych eliptycznych przy tworzeniu kryptosystemów asymetrycznych (obecnie wypierają one klasyczne krypto systemy typu RSA). Następnie została opisana metoda szyfrowania dynamicznego ZT-UNITAKOD. W ostatnim punkcie przedstawiono zjawisko phishingu oraz omówiono sposoby obrony przed nim.

1. Raport CERT

W ostatnich latach co raz większego znaczenia w działalności poszczególnych przedsiębiorstw, jak i szeroko rozumianej gospodarki, nabiera sieć internetowa. W związku z tym ważne jest zapewnienie bezpieczeństwa podczas korzy-

stania z tego medium. W Polsce analizą zjawisk związanych z bezpieczeństwem internetowym zajmuje się CERT (Computer Emergency Response Team). CERT Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo internetowe. CERT Polska działa od 1996 r. (do końca roku 2000 pod nazwą CERTNASK), a od roku 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams). W ramach tego forum współpracuje z podobnymi organizacjami na całym świecie.

Do głównych zadań zespołu należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci,
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń,
- współpraca z innymi zespołami (Incidents Response Team) w ramach FIRST,
- prowadzenie działań zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego,
- prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu,
- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego,
- prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów, a także klasyfikacji i tworzenia statystyk [www 2].

W kwietniu 2013 r. zespół przedstawił analizę incydentów naruszających bezpieczeństwo teleinformatyczne w roku 2012. Można ją znaleźć na [www 2]. Najważniejsze obserwacje podsumowujące raport podane są poniżej:

- w 2012 r. CERT Polska odnotował ponad 10,5 mln automatycznych zgłoszeń dotyczących naruszeń bezpieczeństwa,
- po raz pierwszy od 2005 r. wzrosła liczba incydentów obsłużonych przez CERT Polska ręcznie, a więc tych najpoważniejszych; w 2012 r. było ich 1082, czyli o blisko 80% więcej niż przed rokiem – głównie za sprawą złośliwego oprogramowania i phishingu,
- Polska wypada dobrze na tle innych krajów pod względem liczby utrzymywanych w naszym kraju stron związanych z phishingiem i złośliwym oprogramowaniem – w statystykach jest poza pierwszą dziesiątką (znacznie gorzej jest w przypadku problemów związanych z komputerami użytkowników indywidualnych, a więc liczby botów, skanowań i wysyłanego spamu),
- najwięcej zgłoszeń botów, a więc zainfekowanych komputerów, sterowanych centralnie przez specjalne kontrolery, dotyczyło trzech rodzajów złośliwego oprogramowania: Viruta, DNSChangera oraz różnych odmian ZeuSa (średnio 8000 botów dziennie),
- nastąpił systematyczny wzrost liczby incydentów związanych z phishingiem – zarówno w tradycyjnej formie, polegającej na tworzeniu stron podszywają-

cych się pod banki, sklepy internetowe itp., jak i związanego ze złośliwym oprogramowaniem potrafiącym modyfikować zawartość stron bankowych odwiedzanych przez użytkownika,
- najczęściej atakowaną usługą w przypadku skanowań jest niezmiennie SMB w Microsoft Windows (445/TCP),
- nowością wśród często atakowanych usług jest Zdalny Pulpit w systemach MS Windows (3389/TCP),
- znacząco, bo aż o 56%, powiększyła się liczba serwerów DNS w polskich sieciach, które skonfigurowane są w nieprawidłowy sposób, narażając na niebezpieczeństwo wszystkich użytkowników sieci (powodem jest głównie brak świadomości istnienia problemu u ich administratorów),
- w zgłoszeniach trafiających do ręcznego systemu obsługi wzrasta przewaga tych pochodzących z zagranicznych podmiotów komercyjnych nad zgłoszeniami od osób prywatnych z Polski.

2. Długość klucza a bezpieczeństwo internetowe

Kryptografia klucza publicznego i bezpieczne systemy wymiany kluczy są obecnie podstawą bezpieczeństwa bankowości elektronicznej, zapewniają zdalne aktualizowanie systemów operacyjnych czy wysyłanie poufnych e-maili. Należą do nich algorytmy RSA lub Diffiego–Hellmana (do tej pory największym kluczem, gdy idzie o system RSA, jaki został rozłożony na czynniki pierwsze, jest klucz 768-bitowy; stało się to na przełomie 2009 i 2010 r.). Długość klucza kryptosystemu wpływa zatem na jego odporność na atak. Można to zobaczyć na [www 3]. W poniższej tabeli są szczegóły.

Tabela 1. Długości kluczy systemów z kluczem publicznym

System	Przewidywana odporność na atak (lata)	Długość klucza wersji RSA (w bitach)	Długość klucza wersji opartej na krzywych eliptycznych (w bitach)	Długość funkcji haszującej (w bitach)
Lenstra/Vertheul	do 2013	1513	151	160
Lenstra Updated	do 2013	1191	154	154
Ecrypt II	do 2015	1248	160	160
NIST	do 2030	2048	224	224
ANSSI	do 2020	2048	200	200
BSI	do 2015	1976	224	224
NSA Suite B	bd.	nie rekomenduje tej wersji	384	384
Network Working Group RFC 3766	bd.	1491	164	164

Źródło: Na podstawie [www 3].

Na podstawie danych zawartych w powyższej tabeli wydaje się, że nadchodzi jednak schyłek kryptografii bazującej na liczbach pierwszych. Dowodem na to jest brak rekomendacji dla kryptosystemów RSA i Diffiego–Hellmana przez amerykańską Agencje Bezpieczeństwa Narodowego (NSA), w wydanym przez nią w roku 2005 pakiecie algorytmów Suite B. Prawdopodobnie dotyczy to także zestawu NSA Suite A, opracowanego do zabezpieczania informacji o najwyższym poziomie tajności, o którym oficjalnie bardzo mało wiadomo. Kolejną przesłanką za takim wnioskiem jest praca [Joux, 2013]. Wynika z niej istnienie efektywnych algorytmów znajdywania logarytmu dyskretnego w ciałach skończonych (czyli możliwość łamania kryptosystemów bazujących na liczbach pierwszych).

3. Kryptosystemy oparte na krzywych eliptycznych

W punkcie tym omówimy ogólną koncepcję asymetrycznego kryptosystemu bazującego na dodawaniu punktów krzywej eliptycznej [Blake, Seroussi i Smart, 2004; Wilkowski, 2009]. Począwszy od około roku 1985 teorię krzywych eliptycznych, perełkę matematyki XIX w., nad ciałami skończonymi stosowano do różnych problemów kryptograficznych, jak rozkład liczb naturalnych na czynniki pierwsze, testy pierwszości czy konstrukcja kryptosystemów asymetrycznych. Grupy punktów krzywych eliptycznych nad ciałami skończonymi są podobne do grup multiplikatywnych ciał skończonych. Mają jednak nad nimi dwie przewagi: jest ich o wiele więcej i wydaje się, że zapewniają ten sam stopień bezpieczeństwa przy mniejszej długości kluczy (co przedstawia tabela 1). Ma to znaczenie w zastosowaniach, które wymagają bardzo wysokiej wydajności (algorytm RSA jest stosunkowo wolny).

Definicja 1. Krzywą eliptyczną E , nad ciałem K, nazywamy zbiór

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b \,;\, a, b \in K\} \cup \{0_E\}, \qquad (1)$$

gdzie: 0_E – **punkt w nieskończoności**, wielomian po prawej stronie nie ma pierwiastków wielokrotnych, charakterystyka ciała K jest różna od 2 i od 3.

Przypomnijmy tutaj, że ciała nieskończone $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ mają charakterystykę równą 0, a ciała skończone F_q , mające $q = p^j$ elementów, lub ciała $\mathbb{Z}/p\mathbb{Z}$, gdzie p jest liczbą pierwszą, są charakterystyki p. Gdy charakterystyka ciała K jest

równa 2 bądź 3, równanie występujące w powyższej definicji ma nieco inną postać, ale tym przypadkiem nie będziemy się zajmować.

Przykład 1 [Yan, 2006]. Niech E będzie krzywą eliptyczną $y^2 = x^3 + 3x$ nad ciałem F_5 . Wówczas krzywa E składa się z 10 punktów:

$$E(F_5) = \{0_E, (0,0), (1,2), (1,3), (2,2), (2,3), (3,1), (3,4), (4,1), (4,4)\} .$$

W poniższej tabeli podane są krzywe nad ciałem F_5 oraz ilość ich punktów.

Tabela 2. Liczba punktów krzywych eliptycznych nad ciałem skończonym

Krzywa eliptyczna	Liczba punktów
$y^2 = x^3 + 2x$	2
$y^2 = x^3 + 4x + 2$	3
$y^2 = x^3 + x$	4
$y^2 = x^3 + 3x + 2$	5
$y^2 = x^3 + 1$	6
$y^2 = x^3 + 2x + 1$	7
$y^2 = x^3 + 4x$	8
$y^2 = x^3 + x + 1$	9
$y^2 = x^3 + 3x$	10

Źródło: Na podstawie [Yan, 2006; Wilkowski. 2009].

Jak wynika z tabeli, liczba elementów krzywej znajduje się między 2 a 10. W ogólnym przypadku prawdziwe jest oszacowanie.

Twierdzenie 1 [Koblitz, 1987].

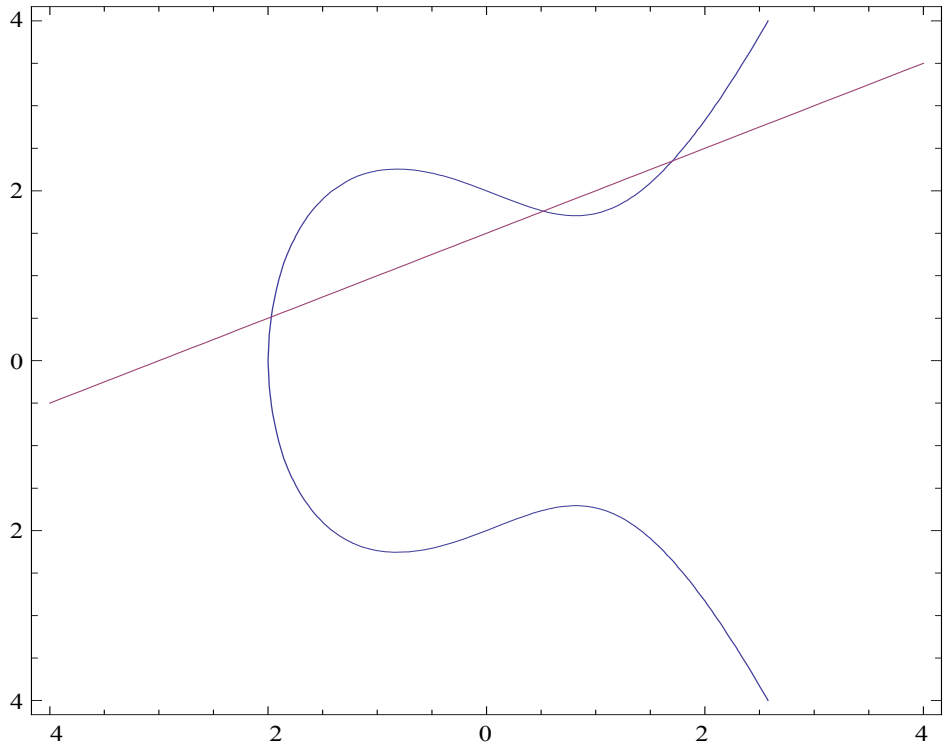
$$\left|E(F_p)\right| \leq 1 + p + 2\sqrt{p} . \tag{2}$$

Przykład 2. Weźmy krzywą eliptyczną $E(\mathbb{R})$ (ma nieskończoną ilość punktów) i prostą ją przecinającą, danymi wzorami:

$$E(\mathbb{R}) = \{(x, y) \in \mathbb{R}^2 : y^2 = x^3 - 2x + 4\} \cup \{0_E\} ,$$

$$y = \frac{1}{2}x + \frac{3}{2} .$$

Przedstawia je poniższy rysunek.



Rys. 1. Krzywa eliptyczna $y^2 = x^3 - 2x + 4$ i prosta $y = \frac{1}{2}x + \frac{3}{2}$

Z powyższego widać, że każda prosta nierównoległa do osi y może przecinać krzywą w trzech punktach (punkt styczności liczymy podwójnie). Dla tej krzywej punkt w nieskończoności 0_E, powinien być wyobrażony jako punkt położony nieskończenie daleko na osi *y*, w kierunku granicznym coraz bardziej stromych stycznych do krzywej, jest on „trzecim punktem przecięcia" każdej prostej pionowej, przecinającej lub stycznej do krzywej *E*, z tą krzywą. Podstawowym działaniem na krzywej eliptycznej jest dodawanie jej punktów. W celu określenia tego działania wygodnie posłużyć się intuicją geometryczną, korzystając z rysunku 1. Wtedy regułę dodawania punktów krzywej eliptycznej można streścić następująco:

suma trzech punktów, w których prosta przecina krzywą wynosi 0_E.

Geometryczne prawo dodawania punktów pozwala łatwo zobaczyć, jak dodać dwa punkty na krzywej eliptycznej, żeby otrzymać trzeci punkt. Aby takie działania wykonywać numerycznie potrzebne są wzory algebraiczne. Niżej przedstawiamy wzory ogólne, prawdziwe w przypadku dowolnych ciał charakterystyki różnej od 2 i od 3.

Niech $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b ; a, b \in K \cup 0E\}$.

Wówczas:

$$P + Q = \begin{cases} 0_E, jeżeli\ x_1 = x_2\ oraz\ y_1 = -y_2, \\ (x_3, y_3), w\ pozostałych\ przypadkach, \end{cases} \tag{3}$$

gdzie:

$$(x_3, y_3) = (d^2 - x_1 - x_2, d(x_1 - x_2) - y_1) \in E(K) ,$$

oraz

$$d = \begin{cases} \dfrac{3x_1^2 + a}{2y_1}, jeżeli\ P = Q, \\ \dfrac{y_2 - y_1}{x_2 - x_1}, w\ pozostałych\ przypadkach. \end{cases} \tag{4}$$

Dodawanie punktów krzywej eliptycznej *E* tworzy w niej strukturę grupy abelowej z elementem neutralnym 0_E. W roku 1922 Mordell udowodnił [za: Miller, 1986], że grupa abelowa punktów dowolnej krzywej eliptycznej nad ciałem liczb wymiernych *Q*, jest sumą prostą skończonej podgrupy złożonej z punktów skończonego rzędu (podgrupy torsyjnej) i podgrupy generowanej przez skończoną liczbę punktów nieskończonego rzędu. Własność ta umożliwia wykorzystanie krzywych eliptycznych w kryptografii. Ważną rolę odegrały tutaj prace [Miller, 1986; Koblitz, 1987]. Od tego momentu krzywe eliptyczne są wnikliwie badane dla potrzeb kryptografii, powstało wiele bardziej bezpiecznych schematów szyfrowania i podpisów cyfrowych, stosowanych często w Internecie. Obecnie kryptografia wykorzystująca te krzywe jest standardem (kanadyjska firma komputerowa Certicom dzierży prym w opracowywaniu kryptograficznej technologii wykorzystującej krzywe eliptyczne – posiada ponad 130 patentów z tym związanych). Podstawowymi cegiełkami, z których jest zbudowany kryptosystem oparty na krzywej eliptycznej *E*, nad ciałem skończonym F_q , są obliczenia sum postaci $P + P + ... + P = kP$, gdzie *P* jest punktem krzywej *E*, a *k* jest liczbą całkowitą. Okazuje się, że można to wykonać, stosując operację powtarzalnego podwajania, za pomocą $O(log_2 k (log_2 q)^3)$ operacji bitowych (jest to zatem szybki algorytm, można go używać w praktyce obliczeniowej). Bezpieczeństwo takiego kryptosystemu opiera się na fakcie, że mając daną krzywą *E*, punkt *P*, należący do niej, oraz punkt *kP* tej krzywej, trudno jest znaleźć liczbę całkowitą *k*. Jest

to **problem logarytmu dyskretnego** na krzywej eliptycznej. Obecnie uważa się, że dla dobrze wybranej krzywej E oraz ciała F_q , rozwiązanie problemu logarytmu dyskretnego w $E(F_q)$ ma złożoność obliczeniową zależną wykładniczo od rozmiaru ciała (zatem algorytmy to umożliwiające nie mają praktycznego znaczenia).

Przykład 3. Prawie każdy kryptosystem z kluczem jawnym, stosowany obecnie w sieci, posiada swój odpowiednik dla krzywych eliptycznych. Przedstawimy teraz odpowiednik kryptosystemu ElGamala [Yan, 2006; Wilkowski, 2009]:

- Alicja i Bartek ujawniają publicznie wybór krzywej eliptycznej E nad ciałem F_q , gdzie $q = p^j$ i p jest dużą liczbą pierwszą, oraz losowy punkt $P \in E$,
- Alicja wybiera losowo liczbę całkowitą r_A (klucz prywatny Alicji) i wyznacza punkt $r_A P$ (klucz jawny Alicji); Bartek także losowo wybiera liczbę całkowitą r_B (klucz prywatny Bartka) i wyznacza punkt $r_B P$ – klucz jawny Bartka (liczby r_A, r_B są tajne, a punkty $r_A P$ oraz $r_B P$ powszechnie znane),
- aby wysłać Bartkowi wiadomość – punkt M, Alicja losowo wybiera liczbę całkowitą k (tajną) i przesyła parę punktów $\big(kP, M + k(r_B P)\big)$,
- aby przeczytać wiadomość M, Bartek oblicza $M + k(r_B P) - r_B(kP)$.

Bartek wysyłając wiadomość Alicji postępuje analogicznie. Każdy użytkownik sieci zna krzywą eliptyczną E, punkt P oraz klucze jawne Alicji i Bartka, może zatem wysyłać do nich zaszyfrowane wiadomości. Osoba podsłuchująca, aby rozszyfrować komunikat, musi umieć radzić sobie z obliczeniem logarytmu dyskretnego na krzywej E. Ale jak wiadomo, nie jest znana efektywna metoda obliczania tych logarytmów, zatem opisany system jest bezpieczny.

Przykład 4. Pośród algorytmów pakietu SuiteB (tabela 1), rekomendowanego przez NSA, są kryptosystemy oparte na krzywych eliptycznych. W dokumentcie NSA [2010], w którym podano przykładowe parametry krzywej oraz startowy punkt P, będące podstawą bezpiecznego kryptosystemu. Współczynniki a, b ze wzoru (1) w definicji 1 są równe:

$a = 2^{521} - 4 =$ 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148,

$b =$ 1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984.

Przy tworzeniu algorytmu bazującego na krzywej eliptycznej ważny jest wybór punktu startowego *P*. W tym przypadku ma on współrzędne:

$$P = (x_P, y_P),$$

gdzie:
x_p = 266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6,

y_p = 375718002577002046354550722449118360359445513476976248669456777961554447744055631669123440501294553956214444453728942852258566672919658081012434427757837678 4.

Rząd punktu *P* (to także rząd grupy punktów krzywej o parametrach *a*, *b*) jest wtedy równy *q*, gdy:
q = 686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700544 9.

Na zakończenie tego punktu warto wspomnieć o kryptografii kwantowej, leżącej na pograniczu klasycznej kryptografii i mechaniki kwantowej. Jej narzędziem jest hipotetyczny komputer kwantowy [Monroe, Wineland, 2008], rozumiany jako układ fizyczny, zaprojektowany tak, aby wynik jego ewolucji, zgodnie z prawami mechaniki kwantowej, reprezentował rozwiązanie określonego problemu obliczeniowego. Przy użyciu takiego komputera możliwe jest „prawdziwie losowe" generowanie liczb losowych [Mitra, 2009] lub rozłożenie liczby naturalnej *N* na czynniki pierwsze w czasie rzędu $O((\log_2 N)^3$ i pamięci $O(\log_2 N)$. Propozycja odpowiedniego algorytmu jest w pracy [Shor, 1996]. Oznaczałoby to koniec kryptosystemów typu RSA. W 2011 r. kanadyjska firma D-Wave zaprezentowała maszynę D-Wave One, określaną jako pierwszy na świecie komputer kwantowy. Wyniki eksperymentów z użyciem tej maszyny można znaleźć w pracy [Boixo i in., 2013]. C. McGeoch i C. Wang to uczeni, którzy po raz pierwszy zdołali porównać ze sobą możliwości komputerów kwantowych i klasycznych w rozwiązywaniu problemów optymalizacji. W swoim artykule [2013] opisują eksperymenty, w których wykorzystano komputer kwantowy D-Wave Two. Wyniki testów pokazały, że dla tych problemów optymalizacji, które można uruchomić bezpośrednio na kwantowych procesorach, maszyny D-Wave okazały się ponad cztery tysiące razy szybsze od rozwiązań software'owych. Gdy chodzi o kla-

syczne problemy algebry liniowej, przy pomocy komputera kwantowego udało się rozwiązać układ dwóch równań z dwiema niewiadomymi [Cai i in., 2013]. Jak podają autorzy wymienionej pracy, właściwe rozwiązanie znajdywane jest średnio dziewięć razy na dziesięć prób, ale jak na razie, jest to immanentna cecha komputerów kwantowych.

4. Metoda ZT-UNITAKOD

W punkcie tym omówimy kryptosystem mogący zwiększyć bezpieczeństwo teleinformatyczne. Powstał on na Politechnice Wrocławskiej na początku lat XXI w. Opiera się na koncepcji szyfrowania dynamicznego [Juzwiszyn, Wilkowski, 2005]. Dotychczas każdy używany kryptosystem posiadał:

- tabelę przyporządkowania,
- stały, tajny klucz wymagający tworzenia, ochrony, przechowywania, przesyłania,
- całością kierował człowiek.

W metodzie ZT-UNITAKOD [Topolewski, 2002] nie obowiązują powyższe reguły. Nie ma tabeli przyporządkowania (każdy znak przyjmuje losowo jedną z 256 możliwych postaci i za każdym razem inną postać), ani stałego tajnego klucza. Ograniczona została również decydująca rola człowieka w systemie ochrony informacji. Jest ona oparta wyłącznie na generatorach permutacji oraz modelach matematycznych tworzących jednorazowy klucz dynamiczny. Wynika z tego, że szyfr zmienia się wraz ze zmianą daty i czasu (w praktyce co 1 sekundę). Metoda ta jest chroniona patentem w USA (nr 08/775, 253-SYSTEM AND METHOD ZT-UNITAKOD FOR ENCRYPTING AND DECRYPTING DATA), informacje o niej można znaleźć na [www 4]. Model matematyczny szyfru:

$$Szyfr = A + B(mod256), \tag{5}$$

gdzie A jest tablicą kryptograficzną, jednorazowym kluczem dynamicznym (to po prostu macierz o 256 wierszach i 256 kolumnach zmieniająca się wraz ze zmianą czasu), natomiast B to przesyłany tekst jawny. Model deszyfracji jest następujący :

$$B = S - A(mod256)\text{ , dla } S - A \geq 0, \tag{6}$$

$$B = (S - A) + 256(mod256)\text{ , dla } S - A \leq 0. \tag{7}$$

W celu utworzenia tablicy kryptograficznej A, wykorzystuje się dwa generatory permutacji:

- generator multiplikatywny $G_1 = cx_i(mod256)$, gdzie c to liczby nieparzyste od 3 do 255,
- generator mieszany $G_2 = ax_i + b(mod256)$, gdzie a to liczby nieparzyste od 1 do 255 spełniające równanie $a = 1(mod4)$, b są liczbami nieparzystymi od 1 do 255.

Tablica kryptograficzna ma 256 wierszy i kolumn. Zatem A składa się z 65 536 bajtów. Liczba możliwych permutacji wynosi $(256!)^{256}$.

Taka jest potencjalna moc kryptosystemów opartych na metodzie ZT-UNITAKOD (większa niż obecnie stosowanych systemów typu RSA).

Wydaje się, że do przesyłania oprogramowania kryptosystemów opartych na metodzie ZT-UNITAKOD w sieciach należy posługiwać się powszechnie dostępnymi algorytmami asymetrycznymi (np. bazującymi na krzywych eliptycznych). Kodowanie dynamiczne jest optymalnym rozwiązaniem w przypadku przesyłania ważnych informacji między niewielką liczbą użytkowników (wyżsi urzędnicy, prezesi banków, w dyplomacji czy wojskowości) oraz szyfrowania baz danych. Należy przypuszczać, że metody oparte na kodowaniu dynamicznym łącznie z kryptosystemami bazującymi na funkcjach jednokierunkowych będą coraz bardziej rozwijane i rozpowszechniane.

5. Phishing

W punkcie tym omówimy sposoby zabezpieczenia się użytkownika sieci przed przestępstwem internetowym, jakim jest phishing [Cranor, 2009; Wilkowski, 2009]. Zajmuje on poczesne miejsce wśród wniosków podsumowujących raport CERT przedstawionych w pkt. 1. Za Wikipedią rozumiemy przez to wyłudzanie poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne. Jest to rodzaj ataku opartego na inżynierii społecznej. „Termin został ukuty w połowie lat 90, przez crackerów próbujących wykraść konta w serwisie AOL (duży dostawca usług internetowych w USA). Atakujący udawał członka zespołu AOL i wysyłał wiadomość do potencjalnej ofiary. Wiadomość zawierała prośbę o ujawnienie hasła, np. dla »zweryfikowania konta« lub »potwierdzenia informacji w rachunku«. Gdy ofiara podawała hasło, napastnik uzyskiwał dostęp do konta i wykorzystywał je w przestępczym celu, np. do wysyłania spamu” [www 6] lub w celach zarobkowych. Straty tym spowodowane w USA w roku 2007 wyniosły 3,2 mld dolarów [Cranor, 2009].

Wymieńmy zdroworozsądkowe rady, które każdy internauta może stosować od zaraz, podczas korzystania z sieci:

- w przypadku e-maila z prośbą o odwiedzenie i zalogowanie się na stronie danego serwisu warto potwierdzić autentyczność listu na stronie administratora,
- nie należy otwierać hiperłączy bezpośrednio z otrzymanego e-maila,
- jeśli masz wątpliwości co do adresu witryny, sprawdź go za pomocą wyszukiwarki (fałszywy, w przeciwieństwie do prawidłowego, nie pojawi się na początku listy wyników),
- należy regularnie uaktualniać system i oprogramowanie,
- nie wolno przesyłać mailem żadnych danych osobistych: haseł, numerów kart kredytowych itp.,
- banki i instytucje finansowe stosują protokół HTTPS tam, gdzie konieczne jest zalogowanie do systemu. Jeśli strona z logowaniem nie zawiera w adresie nazwy protokołu HTTPS, powinno się zgłosić to osobom z banku i nie podawać na niej żadnych danych,
- używanie OpenDNS (to darmowy system serwerów oraz protokół komunikacyjny zapewniający zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową),
- nie korzystać z domen mających mniej niż 12 miesięcy,
- nie należy odwiedzać stron zawierających znane logotypy, gdy domena nie należy do ich właściciela,
- podejrzanym parametrem jest URL zawierający @, myślnik, adres IP, bądź więcej niż 5 kropek, lub gdy URL nie odpowiada adresowi wskazanemu przez Google,
- nie należy wchodzić na strony z wyodrębnionym polem do wprowadzania tekstu.

Więcej informacji na ten temat jest w pracy [Cranor, 2009] oraz na [www 1]. Techniki przeciwdziałające łowieniu haseł, opierające się na użyciu haseł jednorazowych, przedstawiono w pracy [Khan, 2013].

Podsumowanie

Specjaliści od bezpieczeństwa internetowego mawiają, że instytucje można podzielić na dwa podzbiory. W jednym są te, które zostały już zaatakowane, w drugim te, które jeszcze o tym nie wiedzą. Należy pamiętać, że w Polsce jest infekowanych w ciągu doby około 280 tys. komputerów osobistych (według raportu CERT). Bardzo ważną rolę w cyberbezpieczeństwie odgrywa zatem człowiek. Teoretyczna skuteczność metod ochrony często jest bliska jedności. Po uwzględnieniu tak

zwanego czynnika ludzkiego spada ona o połowę. Przedstawione we wcześniejszych punktach procedury, stosowane przez pojedynczego użytkownika Internetu, powinny wspierać zbiorowe bezpieczeństwo. Należy je traktować jak zasady higieny osobistej. Nie wszystko jednak zależy tylko od nas. Na zakończenie warto więc wspomnieć słowa Cycerona: *vitam regit fortuna, non sapientia* [Dubiński, 2005].

Literatura

Blake I., Seroussi G., Smart N. (2004), *Krzywe eliptyczne w kryptografii*, Wydawnictwa Naukowo-Techniczne, Warszawa.

Boixo S., Isakov S., Wang Z., Wecker D., Lidar D., Martinis J., Troyer M. (2013), *Quantum Annealing with More than One Hundred Qubits*, 16 April, www.arxiv.org.arXiv: 1304.4595v1 [quant-ph] (dostęp: 19.12.2015).

Cai X.-D., Weedbrook C., Su Z.-E., Chen M.-C., Gu M., Zu M.-J., Li L., Liu N.-L., Lu C.-Y., Pan J.-W. (2013), *Experimental Quantum Computing to Solve Systems of Linear Equations*, "Physical Review Letters", Vol. 110.

Cranor L. (2009), *Czy phishing da się zwalczyć ?* „Świat Nauki" styczeń, nr 1 (209).

Dubiński M. (2005), *Sentencje łacińskie*, Świat Książki, Warszawa.

Joux A. (2013), *Faster Index Calculus for the Medium Prime Case. Application to 1175--bit and 1425-bit Finite Fields*, Cryptology ePrint Archive: Report 2012/720, https://eprint.iacr.org/2012/720.pdf (dostęp: 19.12.2015).

Juzwiszyn J., Wilkowski A. (2005). *Kryptografia dynamiczna*, Wydawnictwo Akademii Ekonomicznej, Wrocław.

Khan A (2013), *Preventing Phishing Attacks Using One Time Password and User Machine Identification*, "International Journal of Computer Applications", Vol. 68, No. 3.

Koblitz N. (1987), *Elliptic Curve Cryptosystems*, "Mathematics of Computation", No. 48.

McGeoch C., Wang C. (2013), *Experimental Evaluation of an Adiabiatic Quantum System for Combinatorial Optimization*, http://graphics8.nytimes.com/packages/pdf/business/quantum-study.pdf (dostęp: 19.12.2015).

Miller V. (1986), *Uses of Elliptic Curves in Cryptography* [w:] *Advances in Cryptology. CRYPTO '85 Proceedings*, Lecture Notes in Computer Science, Vol. 218, Ed. by H.C. Williams, Springer-Verlag, Berlin, s. 417-426.

Mitra A. (2009), *Uncontrollable Random Number Generation Is Possible*, 24 April, www.arxiv.org.arXiv:0904.3677 (dostęp: 19.12.2015).

Monroe Ch., Wineland D. (2008), *Jonowe maszyny cyfrowe*, „Świat Nauki", nr 9(205).

NSA (2010), *Mathematical Routines for the NIST Prime Elliptic Curves*, https://www.nsa.gov/ia/_files/nist-routines.pdf (dostęp: 19.12.2015).

Shor W. (1996), *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, 25 January, www.arxiv.org.arXiv:quant-ph/9508027v2 1996 (dostęp: 19.12.2015).

Topolewski Z. (2002). *Komputerowe zabezpieczenie poufności informacji w zarządzaniu*, Wydawnictwo Continuo. Wrocław

Wilkowski A. (2009), *Elliptic curves and their uses in Internet security.* "Mathematical Economics", No. 5(12).

Yan S. (2006), *Teoria liczb w informatyce*, Wydawnictwo Naukowe PWN, Warszawa.

[www 1] http://apwg.org/advice (19.12.2015).

[www 2] www.cert.pl (19.12.2015).

[www 3] www.keylength.com (19.12.2015).

[www 4] www.perfect-crypt.pl (19.12.2015).

[www 5] https://pl.wikipedia.org/wiki/CERT_Polska (19.12.2015).

[www 6] https://pl.wikipedia.org/wiki/Phishing (19.12.2015).

ON INTERNET SECURITY

Summary: In this paper we present public key cryptosystems. We also talk about cryptosystem which to base on elliptic curve. In 4 part we present how to use ZT-UNITA-KOD method to dynamic code. Finally, we discuss the ways to protect the internet user from phishing.

Keywords: public key cryptosystem, dynamic code, elliptic curve, phishing.