Bartosz Żółtak twórca szyfru VMPC opowiada o swojej przygodzie z kryptologią

Bartosz Żółtak. Autor funkcji jednokierunkowej VMPC, szyfru VMPC oraz aplikacji do szyfrowania danych VMPC Data Security opowiada o historii stworzenia VMPC, o wyjeździe na konferencję do Indii oraz dalszych pracach nad stworzeniem oprogramowania wykorzystującego szyfr VMPC.

Kiedy i jak zaczęła się Twoja przygoda z kryptologią?

W grudniu 1998 roku. Zaczęło się niepozornie. Lubiłem programować i bez wyraźnego powodu wpadł mi pomysł, aby pobawić się w napisanie własnej procedury do szyfrowania danych. Później okazało się, że w tej procedurze - sam nie wiem dlaczego - znalazł się zalążek funkcji jednokierunkowej VMPC.

W jakich okolicznościach odkryłeś podstawy funkcji VMPC?

Znalazły się one już w pierwszej "spontanicznie" napisanej procedurze do szyfrowania danych. Nie wiem czemu, ale wydawało mi się, że tego typu operacja - składanie permutacji z dodatkowymi operacjami arytmetycznymi - może być ciekawa. Było to raczej błądzenie po omacku, przypadek, a nie wynik analiz. Może trochę intuicji. Ale sam dopiero po kilku latach badań zrozumiałem, dlaczego takie przekształcenie jest rzeczywiście ciekawe - wcześniej tego nie widziałem, jedynie tak mi się wydawało :-).

Czemu zawdzięczasz odkrycie funkcji VMPC?

Myślę, że przede wszystkim uporowi. Odkrycie jej to był raczej przypadek. Ale potem przez kilka lat z uporem maniaka analizowałem to przekształcenie. Nie wiem jakim cudem miałem na to ochotę, bo ogólnie jestem raczej leniwy :-). Ale coś w tej funkcji mnie pociągało i analizowanie jej sprawiało mi prawdziwą przyjemność.

Co jest takiego ciekawego w tej funkcji?

Gdy wiemy, że jakaś liczba pomnożona przez 5 daje 10, to wiemy, że tą liczbą jest 2. Umiemy bowiem wykonać operację odwrotną do mnożenia - dzielenie. Z funkcją VMPC jest inaczej. Jeśli wiemy, że 256-elementowa permutacja (np. 25,142,0,84,...,255,84 - po prostu 256 "potasowanych" liczb) jest funkcją VMPC jakiejś innej permutacji, to nie wiemy, jakiej. Ściślej – znalezienie takiej permutacji wymaga ogromnie dużo wysiłku. Dla 256-elementowej permutacji jest to wg obecnie znanych mi analiz 2^260 operacji, a więc około 1000...000 (liczba zawierająca 78 zer) operacji. To naprawdę dużo. Wszystkie komputery na świecie pracujące razem milion lat nie byłyby w stanie tylu operacji wykonać.

W jaki sposób powstał i był testowany szyfr VMPC?

Sama funkcja VMPC to tylko ciekawostka matematyczna. Coś praktycznego możemy z niej uzyskać, jeśli zastosujemy ją np. do szyfrowania danych. Mniej więcej równolegle z analizowaniem samej funkcji testowałem chyba ze 100 różnych sposobów na zastosowanie jej w kryptografii. Były to niezliczone ilości testów statystycznych (ciąg generowany przez taki szyfr powinien "wyglądać" jak liczby losowe) i innych analiz bezpieczeństwa. To już była żmudna praca, która posuwała się małymi kroczkami. Ale udało się po kilku latach uzyskać algorytm, który wg wszelkich prowadzonych analiz był bezpieczny, a jednocześnie był bardzo prosty w budowie - taki był główny cel. Algorytm szyfrowania VMPC można zapisać w kilku linijkach. I również działa on bardzo szybko na komputerach PC.

Czy miałeś wsparcie z uczelni w zakresie pracy nad tym algorytmem?

Trochę tak. Choć projekt prowadziłem samodzielnie. Niewątpliwie zawdzięczam wsparcie Wrocławskiemu Centrum Transferu Technologii przy Politechnice Wrocławskiej.

Jak wspominasz swój wyjazd do Indii na konferencję FSE 2004, na której przedstawiłeś szerokiej publiczności swój szyfr?

To była przygoda życia. Miało to miejsce 5 lat od rozpoczęcia mojej przygody z kryptografią. Gdy startowałem z lotniska we Wrocławiu pamiętam, że uroniła mi się łza. Było to moment, o którym marzyłem przez całe te 5 lat – aż wreszcie nadszedł - leciałem na spotkanie światowej klasy naukowców, aby opowiedzieć im o tym, co wymyśliłem. Była to chwila, ale naprawdę pozostająca w pamięci.

Na konferencji poznałem ludzi osobiście naukowców, o których wcześniej czytałem w książkach czy artykułach. Było to także duże przeżycie. Ludzie, którzy wcześniej byli legendami, teraz stają się rozmówcami, z którymi mogę pogadać zarówno o kryptografii, jak i o indyjskich jedwabnych dywanach. Wszyscy byli bardzo przyjaźni i nastawieni partnersko. A przecież byli to tacy naukowcy, jak Adi Shamir, Jovan Golic, Willi Meier czy David Wagner.

Jak przyjęto na tej konferencji informacje o funkcji VMPC?

Na konferencji prezentowałem zarówno funkcję VMPC, jako podstawowy twór matematyczny z "rodziny", jak i algorytm szyfrowania bazujący na niej, a więc szyfr VMPC. Przyjęcie było bardzo pozytywne. Za sukces uznaję, że nikomu podczas konferencji nie udało się złamać szyfru ani funkcji :-). W kuluarach usłyszałem kilka miły słów, że jest to "ciekawy algorytm" - było to naprawdę przyjemne uczucie i takie chwile sprawiają, że warto było poświęcić każdą godzinę na pracę nad VMPC.

Jak się czułeś, gdy w publicznych mediach było głośno o Twoim algorytmie?

Fakt, w okolicy wyjazdu do Indii sporo było w mediach o tym. Na początku było to ekscytujące. Ale szczerze mówiąc po kilku wywiadach zaczęło mnie to męczyć, bo za każdym razem musiałem opowiadać mniej więcej to samo.

Czy wtedy myślałeś o tym by zawodowo zająć się tematyką kryptologii?

Tak, choć nigdy na 100%. Kryptografia to raczej moja pasja, nie zawód. Na konferencji byłem jedynym prelegentem bez tytułu doktora lub doktoranta. Doktorem dalej nie jestem, choć sympatyczne było to, że na konferencji ludzie, którzy mnie nie znali, zwracali się do mnie na przemian jako "doctor Zoltak" lub "professor Zoltak" :-).

Nie ciągnęło Cię do pracy naukowej na uczelni?

Do pracy naukowej - tak. Na uczelni - nie. Nie lubię biurokracji, procedur. To mnie bardzo ogranicza i czuję się jak w klatce. Nie umiem wtedy twórczo myśleć. Muszę wiedzieć, że nikt niczego ode mnie nie oczekuje, że nie goni mnie żaden termin. Wtedy czuję się wolny i tylko w takich warunkach mogę pracować i coś wymyślić. Nigdy na poważnie nie myślałem o etacie na uczelni.

Czy po publikacjach na temat szyfru otrzymałeś propozycje pracy w polskich lub zagranicznych firm/organizacji?

Nie, propozycji nie było. Ale też nie szukałem, nie wysłałem CV. Myślę, że z takim dorobkiem miałbym szansę się gdzieś załapać. Ale w firmie czy organizacji bałbym się podobnych problemów, jak w przypadku uczelni - oczekiwań, terminów i czułbym się źle, nie byłbym wolny.

Gdybyś miał wymienić *3* główne zalety szyfru VMPC co by to było?

1. prostota
2. szybkość działania
3. bezpieczeństwo

Czy ktoś próbował kryptoanalizy Twojego algorytmu?

Na konferencji poznałem jednego sympatycznego doktoranta, nazywał się Alexander Maximov. Już podczas konferencji przedstawił on projekt, jak można znaleźć słabość statystyczną w szyfrze VMPC (a więc wykazać, że jeśli będziemy obserwować odpowiednio długi ciąg danych generowanych przez szyfr, to zauważymy tam pewne odchylenia od modelu idealnie losowego ciągu liczb). Jednak znalazłem lukę w jego projekcie i niestety (dla niego :-)) pomysł jego legł w gruzach. Alexander okazał się jednak wytrwałym "przeciwnikiem" (jesteśmy dobrymi kumplami) i na konferencji FSE w kolejnym roku (2005) przedstawił nową obserwację, tym razem już prawidłową. Zauważył on, że po obserwacji 18 milionów gigabajtów danych wygenerowanych przez szyfr VMPC da się zaobserwować pewne odchylenie od modelu idealnie losowego. Nie jest to jednak atak dzięki któremu można złamać szyfr.

Na podstawie algorytmu opracowałeś oprogramowanie przeznaczone do szyfrowania informacji. Na co zwracałeś uwagę podczas tworzenia tego oprogramowania?

Aplikacja VMPC Data Security miała zapewniać przede wszystkim perfekcyjny poziom bezpieczeństwa. Z takim założeniem ją tworzyłem. Dzięki niej możemy zaszyfrować pliki, foldery, emaile, a także wygenerować bezpieczne hasła. Niestety przez to dążenie do super-bezpieczeństwa ucierpiała trochę prostota obsługi programu. Ten aspekt został poprawiony w drugiej wersji aplikacji - od marca 2007 dostępna jest bowiem VMPC Data Security 2 - juz znacznie
przyjaźniejsza w obsłudze, ale zapewniająca tak samo wysoki poziom bezpieczeństwa. Więcej o aplikacji można przeczytać na stronie projektu VMPC - www.szyfrowanie.com.

Co wyróżnia Twoje oprogramowanie spośród innego dostępnego na rynku?

Elastyczność i bezpieczeństwo. Opcje Szyfrowanie plików i folderów są zaprojektowane bardzo elastycznie - można szyfrować pojedyncze pliki, całe foldery, wybrane fragmenty folderów, a po zaszyfrowaniu danych możemy dowolnie modyfikować takie zakodowane archiwum. A bezpieczeństwo było priorytetem na każdym etapie tworzenia aplikacji - zarówno na poziomie kryptograficznym, jak i informatycznym - aby np. nigdzie w pamięci czy na dysku nie został ślad klucza ani szyfrowanych danych. Myślę, że każdy, kto ma na dysku dane, które nie powinny się znaleźć w obcych rękach spałby spokojniej, gdyby używał tego typu narzędzia. Wtedy nawet jeśli ktoś wykradnie dane - bez hasła dane te wyglądają jak losowy ciąg liczb i nic z niego nie można odczytać.

Algorytm w kręgach osób zainteresowanych bezpieczeństwem informacji a w szczególności kryptologią wzbudził duże zainteresowanie. Niestety nie zdobył ogólnoświatowej popularności, mimo, iż w wielu elementach przewyższa znane i szeroko stosowane algorytmy kryptograficzne. Jak myślisz dlaczego tak się stało?

Promocja nowego algorytmu szyfrowania to ciężka sprawa. Aby stworzyć algorytm, który stałby się nowym standardem trzeba by pewnie wielkiego lobby wśród naukowców - sam dobry algorytm nie wystarcza. Jest to ogromne przedsięwzięcie.

Jakie są Twoje dalsze plany zawodowe? Czy wiążesz je z kryptologią lub bezpieczeństwem informacji?

Obecnie przede wszystkim zajmuję się promocją aplikacji do szyfrowania danych - VMPC Data Security 2. Pomaga ona zabezpieczać dane już w kilku firmach i mam nadzieję, że będzie ich coraz więcej :-) Szukam także kolejnych dystrybutorów aplikacji. Ostatnio brałem udział we wdrażaniu szyfru VMPC w nowym systemie dystrybucji elektronicznej prasy http://e-kiosk.pl (można tam kupić taniej niż w kiosku już całkiem sporo tytułów) gdzie dzięki VMPC możliwe było zabezpieczenie treści podczas czytania gazet bez podłączenia do internetu.

A marzy mi się przeprowadzenie lub przynajmniej zbliżenie się do dowodu na to, że funkcja VMPC jest jednokierunkowa. Przeprowadzenie takiego dowodu rozwiązałoby jeden z 7 tzw. "problemów milenijnych". Są to zagadnienia matematyczne nierozwiązane od lat. Za rozwiązanie dowolnego z
nich Clay Mathematics Institute w USA ufundował nagrodę w wysokości miliona dolarów. Udowodnienie, że funkcja VMPC jest jednokierunkowa pozwoliłoby rozwiązać problem "P vs NP". Cóż, ale to raczej w sferze marzeń. Choć wierzę, że kiedyś ktoś taki dowód dla funkcji VMPC przeprowadzi, nie wiem tylko, czy nastąpi to za 100 lat, czy wcześniej :-).

Na koniec chciałbym pozdrowić wszystkich czytelników portalu Centrum.Bezpieczenstwa.pl i zachęcić ich do spełniania swoich marzeń i dążenia do obranych celów, nawet gdy wydają się one mało prawdopodobne do spełnienia – z mojego doświadczenia wynika, że naprawdę warto :).

Więcej informacji na temat funkcji i szyfru VMPC znaleźć można w artykule o VMPC w sekcji Artykuły w serwisie lub na stronie www.szyfrowanie.com