Warsaw is cool

Tomasz Kazana

Warsaw Crypto Team

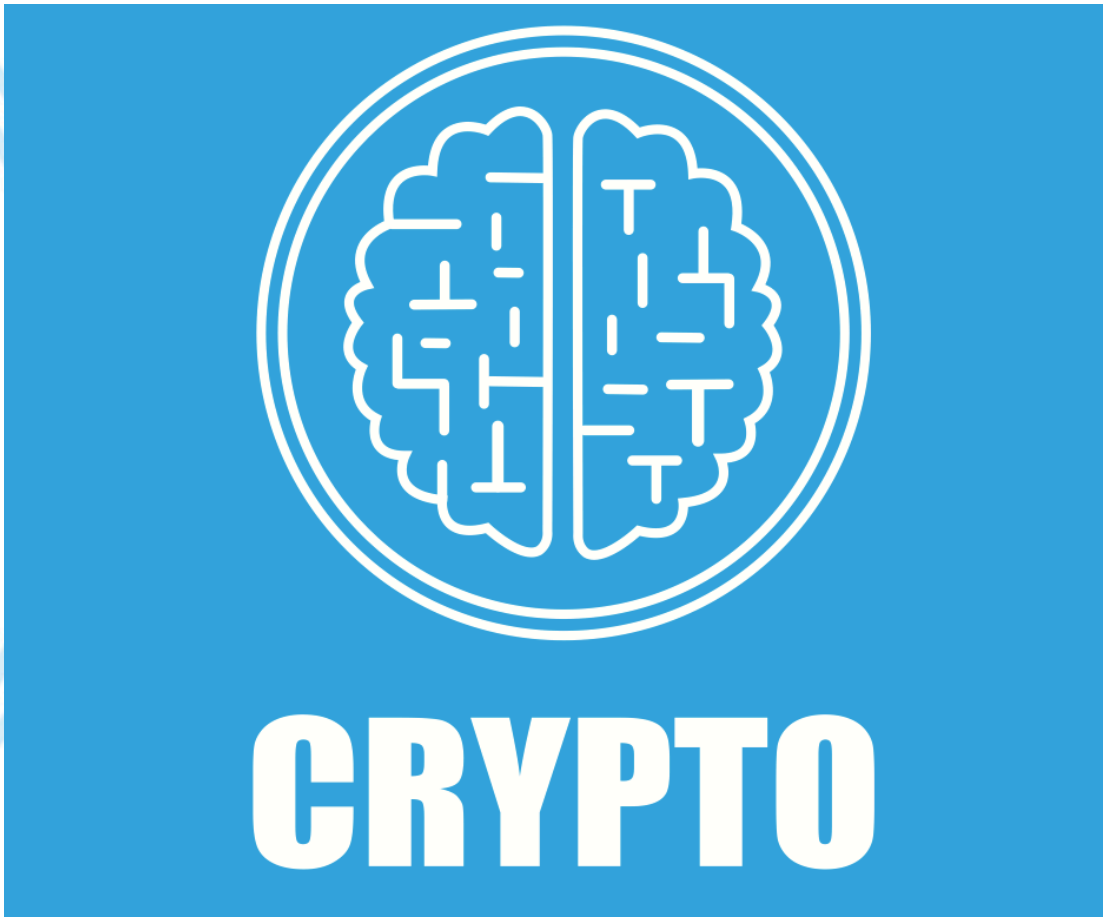
- www.crypto.edu.pl

AGENDA (19 slides!)

- What is really cool we did this year?
- OPEN PROBLEM 1
- Where is Stefan?
- OPEN PROBLEM 2

Our best?

Our best?



OPEN PROBLEM 1

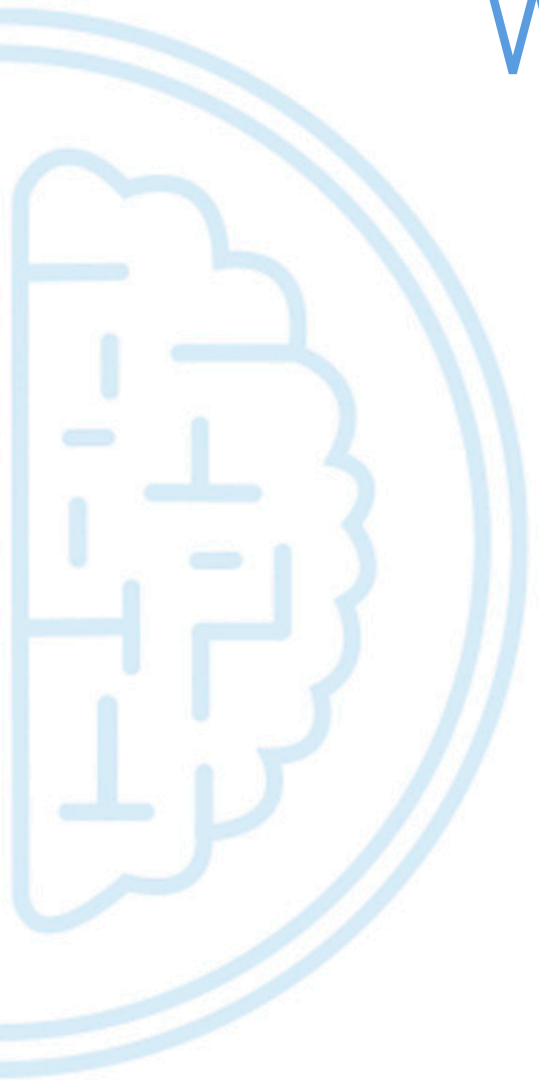
The City: new skyscraper

Daniel Libeskind

Perspective?

OPEN PROBLEM 1
Photoshopped?

Where is Stefan?



Warsaw Crypto HQ

Newspaper

Klucze i rozmowy z kartą

STEFAN DZIEMBOWSKI
Wydział Matematyki, Informatyki i Mechaniki
Uniwersytet Warszawski
crypto.edu.pl/Dziembowski

Dr hab. Stefan Dziembowski jest adiunktem na Wydziale Matematyki, Informatyki i Mechaniki UW oraz na Wydziale Informatyki Uniwersytetu La Sapienza w Rzymie. Pracował naukowo w Danii, we Włoszech i w Szwajcarii. Obecnie kieruje grupą zajmującą się badaniem bezpieczeństwa systemów komputerowych.

Kryptografia służy zabezpieczeniu danych w procesie przesyłania lub gromadzenia. Podstawą tego zabezpieczenia jest szyfr.

Academia: Zajmuje się pan kryptografią, ale też kryptologią. Jaka jest różnica między tymi pojęciami?

Stefan Dziembowski: Kryptologia składa się z kryptografii i kryptoanalizy. Kryptografia zajmuje się tworzeniem szyfrów i systemów kryptograficznych, a kryptoanaliza – ich łamaniem. Ten podział jest trochę sztuczny – wszyscy, którzy zajmują się jednym, zajmują się i drugim.

Porozmawiajmy więc o kryptografii.

To dziedzina rozwijana od czasów starożytnych – już Juliusz Cezar tworzył proste szyfry, żeby kontaktować się z wojskiem. Przez wiele wieków ludzie wymyślali jakiś szyfr, po czym inni go łamali, więc wymyślano nowy albo łatano stary, który ktoś znowu łamał... Ale dopiero w ciągu ostatnich dekad kryptografia stała się nauką. Jej ekspluzja wiąże się z rozwojem informatyki – ona stworzyła język, który pozwolił formalnie mówić na temat bezpieczeństwa.

Właśnie. Czy istnieją szyfry nielamalne?

Każdy szyfr, w którym klucz jest krótszy niż wiadomość, daje się złamać, jeśli tylko ma się dostatecznie dużą moc obliczeniową. Pytanie tylko, czy wydajnie. Jeśli do złamania szyfru trzeba by używać wszystkich komputerów, ja-

Jest na to jakaś rada?

Tak. Kryptografia klucza publicznego. Pomysł jest taki: robimy szyfr, w którym klucz do szyfrowania i klucz do odszyfrowania są inne. Co więcej, klucz do szyfrowania – mój klucz publiczny – mogę ujawnić każdemu. Jeśli ktoś chce wysłać mi wiadomość, szyfruje ją kluczem publicznym, a odtworzyć ją mogę tylko ja, bo tylko ja mam prywatny klucz do odszyfrowania. Oczywiście znajomość klucza publicznego nie może pozwalać na odgadnięcie, jaki jest klucz prywatny.
Podobnie można zrobić z uwierzytelnianiem – mogę wysłać wiadomość, podpisując ją moim kluczem prywatnym, i każdy, kto ma mój klucz publiczny, może sprawdzić, czy wiadomość rzeczywiście pochodzi ode mnie. To się nazywa podpis elektroniczny.

Dotychczas kryptografia kojarzyła mi się z Enigmą i Marianem Rejewskim...

Dr hab. Stefan Dziembowski, magistrantka Katarzyna Janiszewicz i dr Tomasz Kazana z Wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego

robi się komputerowo. Postęp wydajności jest ogromny. Musi tak być, bo z jednej strony zawsze jest ktoś, kto ma skomplikowany, szybko działający system szyfrujący, a z drugiej jest przeciwnik, który chce go złamać. I on również dysponuje dużą mocą obliczeniową. Poza tym wiele szyfrów jest znanych publicznie, a tajność dotyczy wyłącznie klucza. Chodzi o to, że szyfry powinny działać bezpiecznie, nawet jeśli przeciwnik zna ich opis.
Najbardziej znanym szyfrem, który powstał w latach 70., jest Digital Encryption Standard. DES był wykorzystywany przez IBM, przy nie do końca jasnym udziale amerykańskich służb specjalnych. Amerykańska Agencja Bezpieczeństwa Narodowego (National Security Agency; NSA) to instytucja zatrudniająca najprawdopodobniej najwięcej matematyków na świecie. DES, wymyślony przez IBM przy udziale NSA, został opublikowany i stał się standardem amerykańskim i światowym. Przez lata ludzie nie byli pewni, czy DES jest bezpieczny. Czy NSA nie ukryła jakichś „drzwiczek"? Wadą DES jest krótki klucz, oficjalnie długości 64, ale w praktyce 56 bitów. Oznacza to, że liczba kluczy potencjalnych wynosi 2^{56}. Przejrzenie wszystkich

Niestety, już dobrą dekadę temu to 2^{56} stało się osiągalne nawet dla zwykłych ludzi. Teraz już za parę tysięcy dolarów można kupić urządzenie, które łamie DES.
Ale historia tego szyfru nie przestała być ciekawa. Ma on strukturę, która jest logiczna, za wyjątkiem pewnych tajemniczych szczegółów. To tzw. S-boksy. W latach 80. i na początku 90. naukowcy działający w sferze akademickiej opracowali tzw. kryptoanalizę różnicową, która złamała parę szyfrów, ale... z DES sobie słabo radziła, właśnie ze sprawą S-boksów. Wtedy dopiero IBM i NSA przyznały, że znały kryptoanalizy różnicowe już w latach 70., tylko nie chciały ich ujawniać. Kryptografia to więc taka trochę dziwna dziedzina, bo coś odkrywany – my, naukowcy działający na uniwersytetach – i nagle okazuje się, że już 20 lat temu amerykańskie służby specjalne to znały, tylko nie ujawniły.
Na nowy szyfr zrobiono otwarty konkurs światowy. Wygrał projekt belgijski, który jest standardem już od 10 lat – szyfr AES (Advanced Encryption Standard).

Brzmi trochę niepokojąco w kontekście terro-

OPEN PROBLEM 2

Non-malleable codes

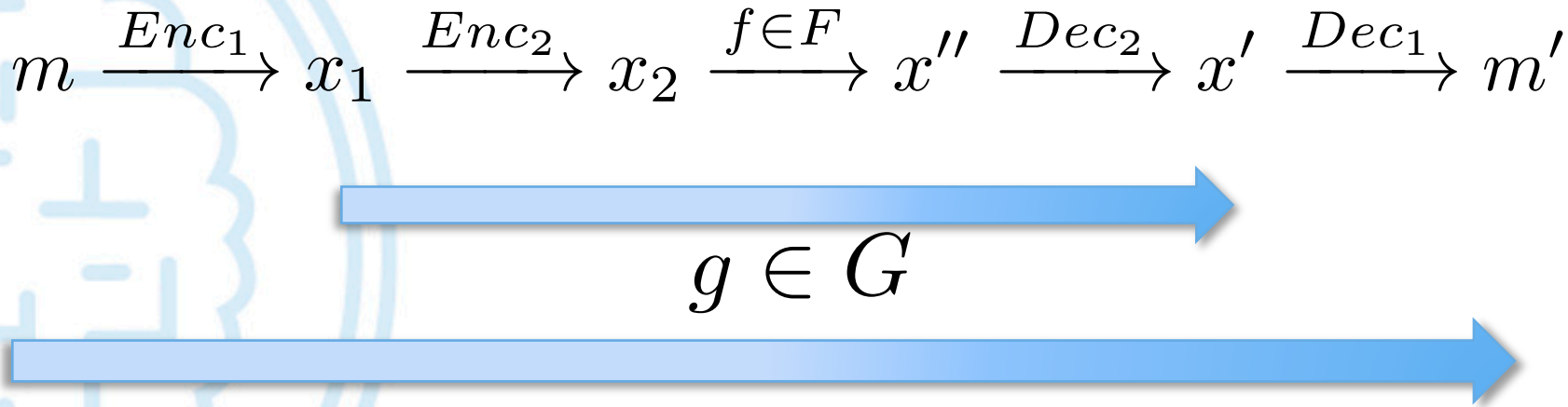
$$m \xrightarrow{Enc} x \xrightarrow{f \in F} x' \xrightarrow{Dec} m'$$

$$g \in G$$

$$G = \{id, constant\}?$$

If so, (Enc, Dec) is non-malleable w.r.t F

Composition



What is G?

Is (Enc_1, Dec_1) non-malleable w.r.t. G?

Aggarval, Dodis, Lovett: cool paper

- F – split model
- G – linear functions over big field

OPEN PROBLEM 2
Better?

- F – as above
- G – linear functions over Z_2