

# Informatikai biztonság alapjai 3. gyakorlat

Oláh Norbert

2024.

# Tartalom

- 1 RSA
  - RSA-séma
- 2 Prímtesztek
  - Prímtesztek
- 3 "A millió kulcsos kérdés" - Az RSA nyilvános kulcsok származásának vizsgálata
- 4 A kulcsforrás észlelése



Ron Rivest; Adi Shamir; Len Adleman

- Az eljárás a nagy számok faktorizációjának problémáján alapul, vagyis hogy egy kellően nagy számról nehéz megállapítani annak prímtényezőit.  
Ha egy szám két igen nagy prímszám szorzata, akkor ennek prímtényezős felbontása még nagyon gyors számítógépekkel is nagyon sokáig tart.
- Számításelméleti okok miatt nem fejthető vissza olyan gyorsan, hogy érdemes legyen megpróbálni.  
Matematikailag nem bizonyított, hogy a titkosított adat visszafejtésére nem létezik kellő gyorsaságú algoritmus, ezért a jövőben ilyen algoritmus felfedezése lehetséges.

# RSA

Nyílt üzenetek halmaza:  $Z_n$   
 ahol  $n = p \cdot q$  (p és q nagy prím)  
 Titkosított üzenetek halmaza:  $Z_n$

# RSA- függvények

- Kulcsgenerálás  
Nyilvános információk:  $n, e$   
Titkos információk:  $p, q, \phi(n), d$   
PK:  $(n, e)$   
SK:  $(n, d)$
- Titkosítás  
Input:  $(M, PK)$   
Output: CT
- Visszafejtés  
Input:  $(CT, SK)$   
Output: M

100

- Választunk két nagy prímet  $p, q$
- RSA modulus kiszámítása  $n=p \cdot q$
- Kiszámítjuk  $\phi(n) = (p - 1) \cdot (q - 1)$   
Választunk 1 véletlen  $e$ :  $1 < e < \phi(n)$   
( $e, \phi(n)$ )=1 relatív prím legyen (kibővített euklideszi algoritmus)
- Kiszámítjuk  $d$ :  $1 < d < \phi(n)$  és  
 $e \cdot d \equiv 1 \pmod{\phi(n)} \rightarrow d$  lineáris kongruencia teljesül ( $d$  ismeretlen)

## RSA- korrektség

## Tények, amikre szükségünk van

- $ed - 1$  a többszöröse  $(p - 1) \cdot (q - 1)$ .
- $a^{p-1} = 1 \pmod p$ , bármely  $p$  prímre. (Kis Fermat tétel)

Cél:

- $m^{ed} = m \bmod p$

Első eset:  $m$   $p$ -nek a többszöröse

- $m = 0 \bmod p$
- $m^{ed} = 0 \bmod p$

Második eset:  $m$   $p$ -nek nem többszöröse

- $m^{ed} = m^{ed-1} \cdot m \bmod p =$
- $m^{\text{multiple of } p-1} \cdot m \bmod p =$
- $m \bmod p$  (Kis Fermat tétel)





\_\_\_\_\_

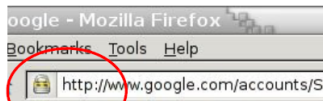
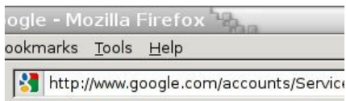
- 1 Az ember a kritikus eleme minden számítógépes rendszernek
  - Az emberek az okai annak, hogy a számítógépek egyáltalán léteznek. :)
- 2 Még ha egy rendszer képes is védekezni egy támadó ellen, az emberek más, kevésbé biztonságos módon is használhatják a rendszert.

1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 2680, 26

- “ , , , ”

# Esettanulmány -Böngésző HTTPS-jelzők

Észrevehető?



Clever favicon inserted  
by network attacker

# Esettanulmány -Böngésző HTTPS-jelzők

## Segítenek az ikonok?


Score	First chose not to enter password...	Group				Total
		1	2	3	1 ∪ 2	
0	upon noticing HTTPS absent	0 0%	0 0%	0 0%	0 0%	0 0%
1	after site-authentication image removed	0 0%	0 0%	2 9%	0 0%	2 4%
2	after warning page	8 47%	5 29%	12 55%	13 37%	25 44%
3	never (always logged in)	10 53%	12 71%	8 36%	22 63%	30 53%
Total		18	17	22	35	57

A felhasználók nem veszik észre az ikonok hiányát!

# Esettanulmány -Böngésző HTTPS-jelzők

## Chrome új verziói

c. 2017

 **Secure** | <https://mail.google.com/mail/u/0/#inbox>

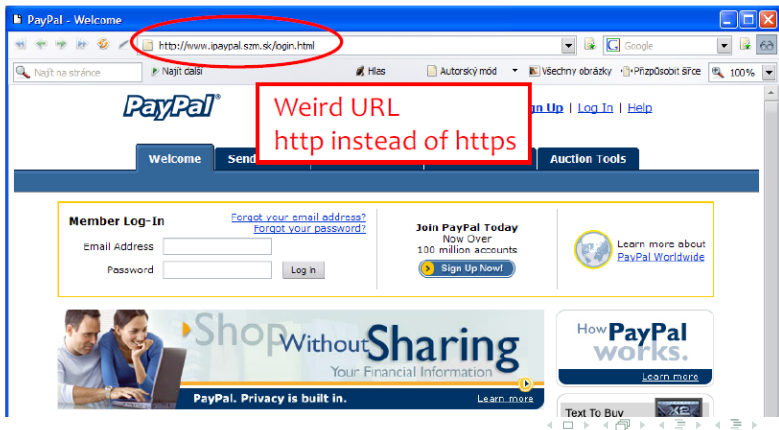
2023

 [mail.google.com/mail/u/1/#inbox](https://mail.google.com/mail/u/1/#inbox)

 **Not Secure** | <https://revoked.badssl.com>

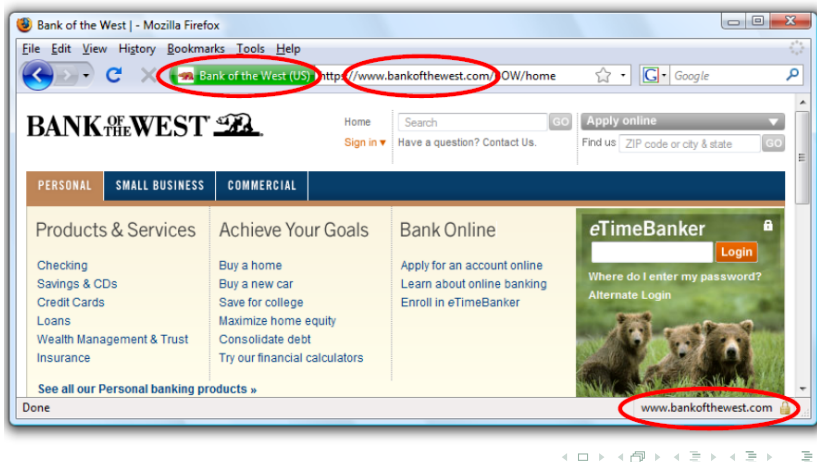
# Esettanulmány -Phishing

Hogyan segít a felhasználóknak elkerülni, hogy bedőljenek az adathalász oldalaknak?



# Esettanulmány -Phishing

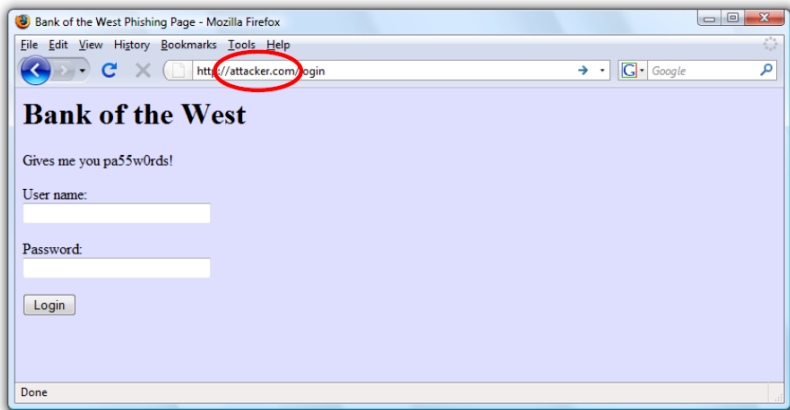
Biztonságos a jelszó beírása?





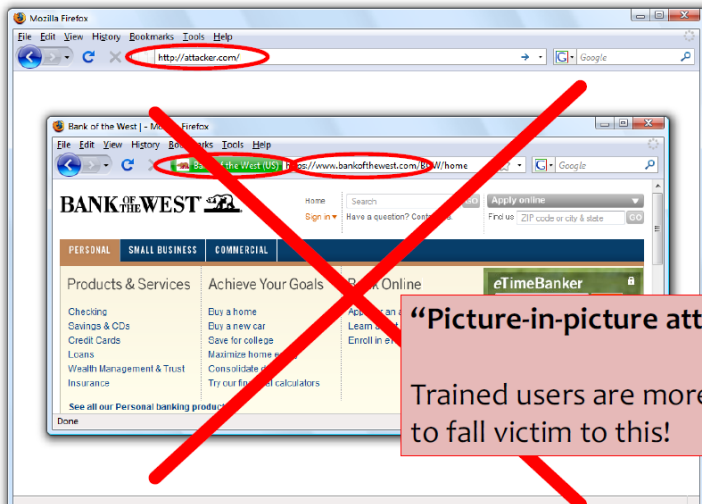
# Esettanulmány -Phishing

Biztonságos a jelszó beírása?



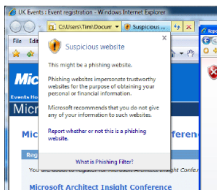
# Esettanulmány -Phishing

Biztonságos a jelszó beírása?

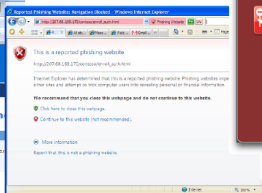


# Esettanulmány -Phishing

- Active warnings significantly more effective
  - Passive (IE): 100% clicked, 90% phished
  - Active (IE): 95% clicked, 45% phished
  - Active (Firefox): 100% clicked, 0% phished



Passive (IE)



Active (IE)



Active (Firefox)

# RSA-visszafejtés

Kínai maradéktétel

Legyenek az  $m_1, \dots, m_k$  modulusok páronként relatív prímek. Ekkor az

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2}$$

...

$$x \equiv c_k \pmod{m_k}$$

szimultán kongruenciarendszer bármilyen  $c_1, \dots, c_k$  egészek esetén megoldható, és a megoldások egyetlen maradékosztályt alkotnak modulo  $m_1 \cdot m_2 \cdot \dots \cdot m_k$ .

# Kínai maradéktétel

Algoritmus:

- $M = m_1 \cdot \dots \cdot m_k$
- $M_i = M/m_i$  ahol  $i = 1, 2, \dots, k$
- Legyen  $y_i$  egész szám az alábbi lineáris kongruencia megoldása  
 $y_i \cdot M_i \equiv 1 \pmod{m_i}$  ahol  $i = 1, \dots, k$
- $x \equiv \sum c_i \cdot y_i \cdot M_i \pmod{M}$

# Kínai maradéktétel példa

$$x \equiv 0 \pmod{5}$$

$$x \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{4}$$

- $M = 5 \cdot 4 \cdot 3 = 60$

- $M_1 = 60/5 = 12$

$$M_2 = 60/3 = 20$$

$$M_3 = 60/4 = 15$$

# Kínai maradéktétel példa

- $12 \cdot y_1 \equiv 1 \pmod{5}$   
 $2 \cdot y_1 \equiv 1 \pmod{5}$   
 $2 \cdot y_1 \equiv 6 \pmod{5}$   
 $y_1 \equiv 3 \pmod{5}$
- $20 \cdot y_2 \equiv 1 \pmod{3}$   
 $2 \cdot y_2 \equiv 1 \pmod{3}$   
 $2 \cdot y_2 \equiv 4 \pmod{3}$   
 $y_2 \equiv 2 \pmod{3}$
- $15 \cdot y_3 \equiv 1 \pmod{4}$   
 $3 \cdot y_3 \equiv 1 \pmod{4}$   
 $3 \cdot y_3 \equiv 9 \pmod{4}$   
 $y_3 \equiv 3 \pmod{4}$

# Kínai maradéktétel példa

- $x \equiv \sum c_i \cdot y_i \cdot M_i \pmod{M}$   
 $x \equiv 0 \cdot 3 \cdot 12 + 1 \cdot 2 \cdot 20 + 2 \cdot 3 \cdot 15 \equiv 130 \equiv 10 \pmod{60}$



# Feladat

Kínai maradéktétel segítségével fejtse vissza a 15 titkosított üzenetet:

$$p = 5$$

$$q = 11$$

$$n = 55$$

$$\phi(n) = 40$$

$$c = 15$$

$$d = 23$$

# Példa

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2}$$

$$c_1 = 15^{23 \pmod{4}} \pmod{5} = 0$$

$$c_2 = 15^{23 \pmod{10}} \pmod{11} = 9$$

$$M_1 = 11$$

$$M_2 = 5$$

$$M = 55$$

$$y_1 \cdot 11 \equiv 1 \pmod{5}$$

$$y_2 \cdot 5 \equiv 1 \pmod{11} \rightarrow \text{kibővített euklideszi algoritmus}$$

# Példa

k	0	1	2	
qk	11	5	1	0
rk	-	2	5	
xk	1	0	1	
yk	0	1	2	

$$y_1 = x = (-1)^2 * 1 = 1$$

$$y_2 = y = (-1)^3 * 2 = -2$$

# Példa

$$x \equiv \sum c_i \cdot y_i \cdot M_i \pmod{M}$$

$$0 \cdot 1 \cdot 11 + 9 \cdot -2 \cdot 5 \pmod{55} = -90 \pmod{55} = 20$$

# Prímtesztek

- $n$  összetettségét vizsgáljuk

- Próbaosztás

Tétel: Ha  $n$  összetett, pozitív egész, akkor létezik  $p \leq \sqrt{n}$  prímosztója.

$n = a \cdot b$ , ahol  $a > 1$  és  $b > 1$

Állítás:  $a \leq \sqrt{n}$  vagy  $b \leq \sqrt{n}$

Indirekt állítás:  $a > \sqrt{n}$  és  $b > \sqrt{n}$

# Prímtesztek

- Állítás:  $a \leq \sqrt{n}$  vagy  $b \leq \sqrt{n}$   
 Indirekt állítás:  $a > \sqrt{n}$  és  $b > \sqrt{n} \rightarrow a \cdot b > n$   
 Legyen  $a \leq \sqrt{n}$  ekkor  $\forall a \in \mathbb{Z}$  esetén  $\exists p|a$  ( $p$  osztója  $a$ -nak)  
 hogy  $p$  prím és  $p \leq a$
- Eratoszthenész szitája (prím számok keresése)  
 2, 3, 4, 5, 6, 7, 8, 9, 10, ...,  $\sqrt{n}$   
 \*, \*, -, \*, -, \*, -, -, -...

# Fermat-teszt

Valószínűségi prímteszt, mely a kis Fermat-tételre alapul ( $a^p \equiv a \pmod p$ ).

- Tétel: Ha  $p$  prím és  $(a, p) = 1$ , akkor  $a^{p-1} \equiv 1 \pmod p$
- Algoritmus:
  - Választok egy  $a$ -t (prím)
  - $a^{p-1} \equiv 1 \pmod p$  ellenőrzése
  - Ha  $a^{p-1} \not\equiv 1 \pmod p \rightarrow p$  összetett

# Álprímek és Carmichael számok

## Definíció:

- Ha  $p$  összetett és  $(a,p)=1$  és  $a^{p-1} \equiv 1 \pmod{p} \rightarrow p$  álprím az  $a$  bázisra nézve
- Ha  $p$  összetett és  $\forall a$  esetén  $(a,p)=1$  és  $a^{p-1} \equiv 1 \pmod{p} \rightarrow p$  Carmichael szám  
(Végtelen Carmichael sok szám van)



# Miller- Rabin teszt

- Legyen  $n$  páratlan pozitív egész szám
- Írjuk fel  $n - 1$ -et a következő alakban  $n - 1 = 2^S \cdot d$ , ahol  $d$  páratlan.
- $d = (n - 1)/2^S$
- Tétel: hogyha  $n$  prím és  $(a, n)=1$  akkor
  - $a^d \equiv 1 \pmod{n}$  vagy
  - $\exists r \in \{0, \dots, S - 1\}$  hogy  $a^{d \cdot 2^r} \equiv -1 \pmod{n}$

# Miller- Rabin példa

- 8 különböző „a” esetén
- $n=561$
- $n - 1 = 2^S \cdot d \rightarrow S = 4$  ( $560/16=35$ )  
 $d = 560/2^4 = 35$
- legyen  $a=2$  ( $a, n$ ) = 1 („a”bázis)  
 $a^d \equiv 1 \pmod{n}$   
 $2^{35} \equiv 1 \pmod{561}$   
 $2^{35} \equiv 263 \pmod{561}$

# Miller- Rabin példa

- $r \in \{0, 1, 2, 3\}$  (S-1-ig megy)
- $2^{(35)^{2^0}} \equiv 263 \pmod{561}$
- $2^{(35)^{2^1}} \equiv 166 \pmod{561}$
- $2^{(35)^{2^2}} \equiv 67 \pmod{561}$
- $2^{(35)^{2^3}} \equiv 1 \pmod{561}$

# Tanúk

## N összetettségének tanúi

- $a \in \{1, 2, 4, 7, 8, 11, 13, 14\}$
- $d=14/2=7;$
- $14 = 2^1 \cdot 7 \rightarrow S = 1$
- $r=0$
- $a^7 \equiv ? \pmod{15}$

# A szerzők céljai

Adhat-e bármilyen információt az RSA nyilvános kulcsainak bitjei?

- Svenda P., Nemec M., Sekan P., Kvasnovskyy R., Formanek D., Komarek D., Matyas V. 2016. The Million-Key Question – Investigating the Origins of RSA Public Keys. In The 25th USENIX Security Symposium (USENIX Security'16). USENIX, p. 893–910.
- 60 millió kulcs elemzése 22 nyitott és zárt forrású könyvtárból és 16 különböző smart kártyából
- Eltérő implementációkból fakadóan nagy pontossággal meg lehet határozni a könyvtárt vagy az intelligens kártyát

A klaszterezés veszélye, hogy

- csökkenti felhasználók anonimitási halmazát,
- gyorsan azonosítható a sebezhető könyvtár kulcsai

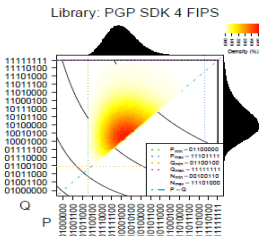
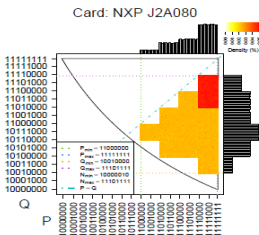
# Prímek eloszlása

Az egyes prímek 8 legmagasabb helyértékű bitjét (MSB) ábrázolták egy hőterképen.

Eredmény:

- Lehetőség van megfigyelni a prím generálási intervallumokat.
- Az MSB minták jelentősen különböztek a kártyák és a szoftverek implementációi tekintetében.
- A minták azonosak voltak az ugyanolyan típusú különböző smart kártyáknál és az egy gyártótól származó néhány típusnál is (valószínűleg a közös kódbázis miatt).
- Az 512 bites kulcsok esetében megfigyelt minták feltehetőleg azonosak az 1024 és a 2048 bites erősebb kulcsokkal (közös kódbázis miatt).

○○



Fehér (nem valószínű) Narancs (sokkal valószínűbb)

# A kulcsforrás észlelése

Intuitív módon az osztályozás a következőképpen működik:

- Azokat modulus biteket, amelyekről tudják, hogy hordozzák a torzítást azonosítják a modulusból származó további bitekkel (egy maszk,  $6 + 3$  bit a módszerükben) .
- A tanulási halmazon adott forráshoz az összes lehetséges maszk kombináció ( $2^9$ ) gyakoriságának kiszámítása.
- Az ismeretlen nyilvános kulcsok osztályozásához a maszk által kiválasztott biteket külön értékként "v" -ként vonják ki
- A legvalószínűbb forrást a v érték legmagasabb kiszámított gyakorisággal rendelkező forrás (2. lépés) azonosítja. Ha ugyanazon forrásból több kulcs található ( $v_i$  több érték), magasabb osztályozási pontosság érhető el az egyes kulcsok valószínűségének elemenkénti szorzásával.



# Side channel attacks

- Mellékcsatornás támadások / Kerülő utas támadások
- ezek nem az algoritmust, hanem annak implementációját támadják
- kivitelezésükhöz a titkosító rendszer nagyon pontos megfigyelésére van szükség
- komoly gyakorlati fenyegetést jelentenek
- cache timing attack: Meltdown és Spectre
- IoT és a kriptovaluta alkalmazások tömegesen használnak RSA kulcspárt

# Az észlelés gyakorlati hatása- Gyenge kulcsok

- Ha valamelyik könyvtár vagy kártya gyenge kulcsokat állít elő, akkor a támadó meg tudja találni a többi kulcsot ugyanazon sebezhető forrásból.
- A kimutatás lehetősége különösen akkor hasznos, ha egy gyenge kulcs elleni sikeres támadás nagy, de gyakorlatilag elérhető összegű számítási erőforrást igényel.
- A potenciálisan sérülékeny kulcsok kiválasztása elősegíti a támadók számára, hogy forrásokat költsenek az összes nyilvános kulcsra.
- A nyilvános modulokból Infineon JCOP 80K kártyákat (512 bit) sikerült az esetek 4.35% faktorizálni Pollard  $p-1$  faktorizációs algoritmusával

Köszönöm a figyelmet!