О способе сокращения перебора в атаке Дюжелла на шифрсистему RSA

Гинятуллин Роман Дамирович.

e-mail: GinRomDam@gmail.com

Студент, Национальный исследовательский ядерный университет «МИФИ»

RSA

Генерация ключа:

Выбираются простые p и q определенной длины;

Находится $n = pq$;

Вычисляется значение функции Эйлера от n:

$$\varphi(n) = (p-1)(q-1);$$

Выбирается e:

$$1 < e < \varphi(n), \qquad (\varphi(n), e) = 1;$$

Вычисляется

$$d\colon\ de \equiv 1\big(\varphi(n)\big);$$

Пара $\{e, n\}$ – открытый ключ,

пара $\{d, n\}$ – секретный ключ.

Атаки на RSA

- На основе алгоритмов разложения на множители
  - Методом Ферма
  - Методом квадратичного решета
  - Методом числового поля
- На основе вычисления дискретного логарифма
  - С использованием свойств открытого ключа
  - Методом Копперсмита
- С использованием свойств секретного ключа
  - Методом Винера
  - Методом Дюжелла (ван Тилборга)

Атака Дюжелла (ван Тилборга)

Верхул и ван Тилборг предложили искать дробь $\frac{k}{d}$ среди дробей вида

$$\frac{rp_{m+1} + sp_m}{rq_{m+1} + sq_m},$$

где $\frac{p_i}{q_i}$ – i-я подходящая дробь для числа $\frac{e}{n}$ и для чисел r и s справедливо:

$$r < \max\left\{\sqrt{2.122(a_{m+3}+2)}(a_{m+2}+1)b, \sqrt{2.122(a_{m+2}+2)}b\right\},$$

$$s < \max\left\{2\sqrt{2.122(a_{m+3}+2)}b, \sqrt{2.122(a_{m+2}+2)}(a_{m+1}+1)b\right\}, b = \frac{d}{n^{0,25}}.$$

Как она работает

Для вычисления нужного m необходимо найти максимальное нечетное m такое, что выполняется неравенство

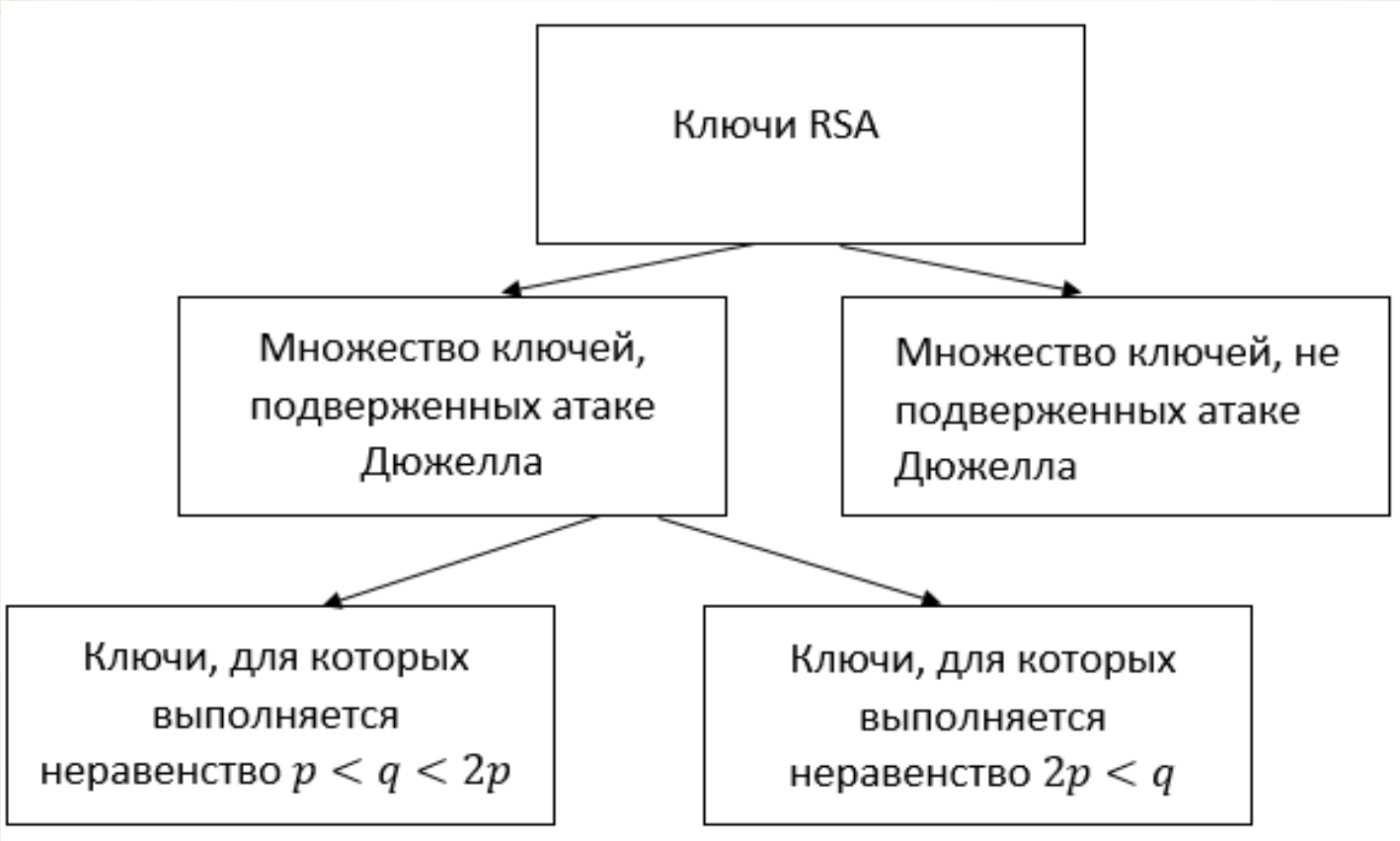
$$\frac{p_m}{q_m} - \frac{e}{n} > \frac{2.122e}{n\sqrt{n}}.$$

Полученное m подставляется в дроби

$$\frac{rp_{m+1} + sp_m}{rq_{m+1} + sq_m}$$

и проверяется, является ли знаменатель полученных дробей секретной экспонентой.

Проведение экспериментов



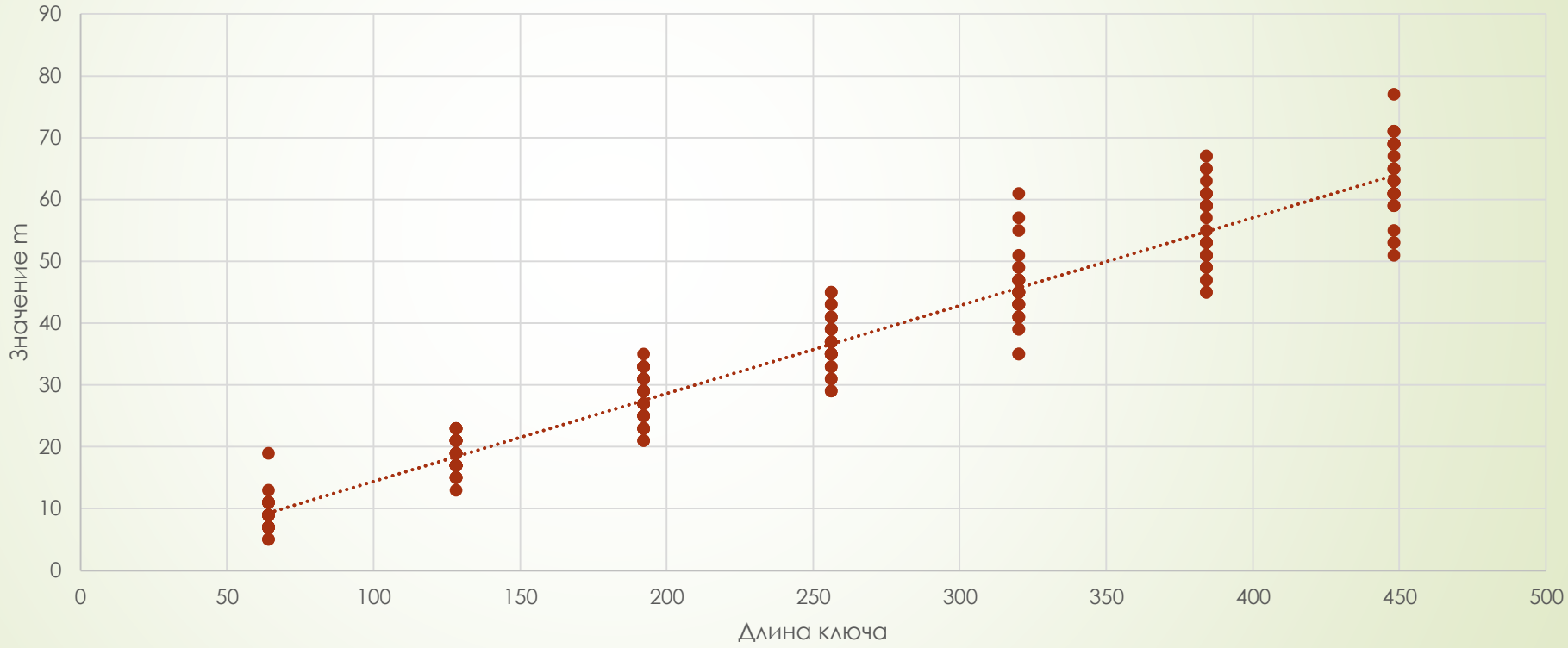
Идея модификация атаки

- Проверить время работы атаки при различных параметрах ключа;
- Проверить выполнение неравенства $\frac{p_m}{q_m} - \frac{e}{n} > \frac{2.122e}{n\sqrt{n}}$ для разных отношений *p* к *q*;
- Определить характер зависимости m от длины ключа.
- Проверить возможно ли повысить нижнюю планку для m;
- Проверить, есть ли зависимость *r* или *s* от ключа.

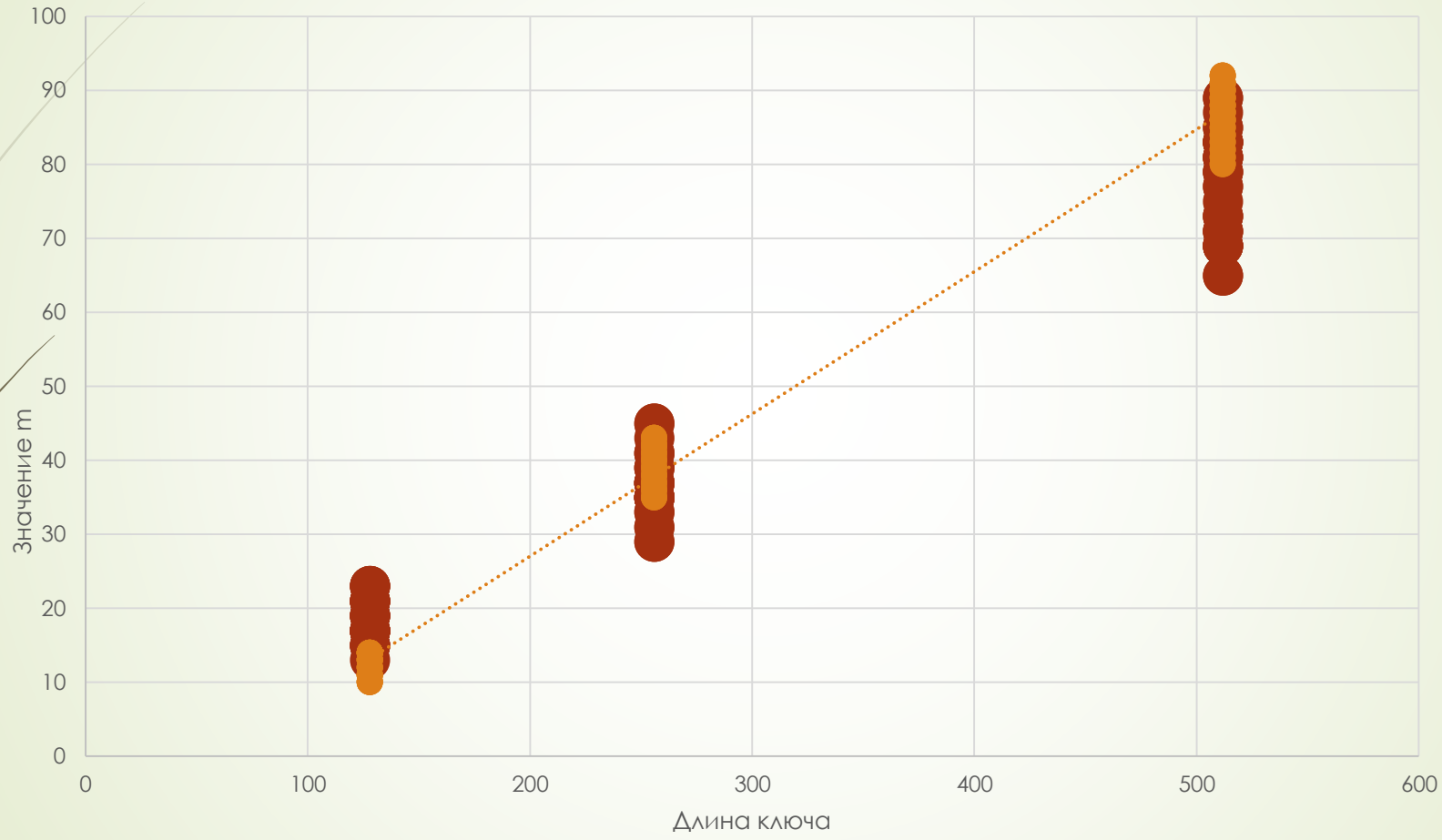
Результаты неоптимизированной атаки при p<q<2p

512 бит			1024 бит			2048 бит		
m	$len\ P$	t	m	$len\ P$	t	m	$len\ P$	t
75	300	32 мин.	141	588	3,5 часа	263	1165	>3 дней
80	316	48 мин.	159	632	4 часа	249	2250	>3 дней
77	304	25 мин.	165	613	2,5 часа	251	1148	~2,5 дня
68	281	55 мин.	151	597	3 часа	239	1175	>3 дней
73	304	32 мин.	147	610	3 часа	257	1095	~ 2 дня
78	309	40 мин.	169	638	2,5 часа	259	1159	2 дня

Значения m


90
80
70
60
50
40
30
20
10
0
Значение m
0
50
100
150
200
250
300
350
400
450
500
Длина ключа

О нужных m



$$\frac{p_m}{q_m} - \frac{e}{n} > \frac{2.122e}{n\sqrt{n}}$$

Есть ли зависимость у *r* и *s*?

Самая «трудозатратная» операция – нахождение r и s:

$$r < \max\left\{\sqrt{2.122(a_{m+3}+2)}(a_{m+2}+1)b, \sqrt{2.122(a_{m+2}+2)}b\right\},$$

$$s < \max\left\{2\sqrt{2.122(a_{m+3}+2)}b, \sqrt{2.122(a_{m+2}+2)}(a_{m+1}+1)b\right\}, b = \frac{d}{n^{0,25}}.$$

Заключение

- Проводилось исследование реализации атаки Дюжелла с целью найти способы оптимизации перебора;
- При $p < q < 2p$ скорость атаки удалось значительно увеличить (в среднем в 15 раз);
- Значения m имеют линейную зависимость от длины ключа, что позволяет сократить перебор и при другом соотношении p и q;
- Зависимости значений r и s от длины ключа не обнаружено.