



## ИССЛЕДОВАНИЕ РАБОТЫ КРИПТОСИСТЕМ И СИСТЕМ УСТАНОВКИ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ

(Казанский национальный исследовательский университет им.  
А.Н.Туполева-КАИ)

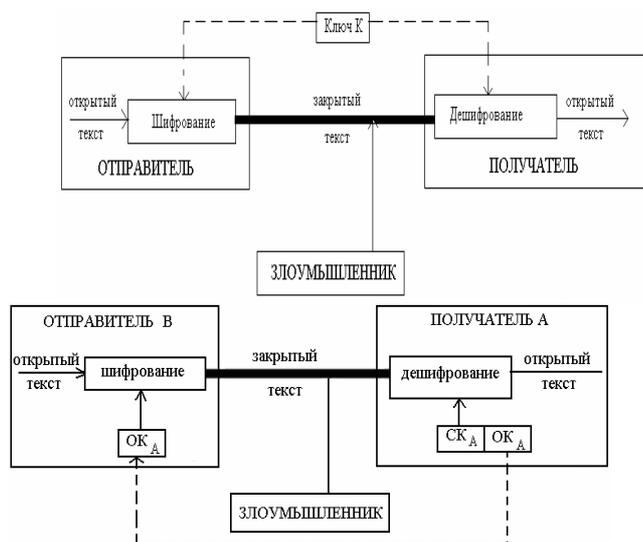
Симметричные криптосистемы применялись задолго до появления электронных информационных технологий.

В данных криптосистемах шифрование и дешифрование информации осуществляется на одном ключе, являющемся секретным. Рассекречивание ключа шифрования ведет к рассекречиванию всего защищенного обмена.

Другим классом криптографических систем являются асимметричные криптосистемы, называемые также криптосистемами с открытым ключом. В асимметричных криптосистемах для шифрования информации используется один ключ, а для дешифрования – другой [2, с. 488].

Целью работы является проведение анализа зашифрованных текстов и определение распространенности символов в них.

Функциональные схемы взаимодействия участников симметричного и асимметричного криптографических обменов приведены на рис. 1.



а) б)

Рис. 1. Функциональная схема:  
а) симметричной криптосистемы;  
б) асимметричной криптосистемы;

При обмене электронными документами по открытым каналам возникает проблема аутентификации автора сообщения и контроля целостности документа. Собственно, сама информация в документе может быть открыта, однако ее изменение может привести к катастрофическим последствиям.



Для обычных, бумажных носителей указанные проблемы решаются путем жесткой привязки информации к физическому носителю, что позволяет использовать для защиты рукописные подписи, печати, водяные знаки и т.д. [3, с. 266]. Для электронных документов эта проблема решается путем привязки к ним особой цифровой последовательности – электронно-цифровой подписи (ЭЦП). Функциональная схема использования ЭЦП приведена на рис. 2.

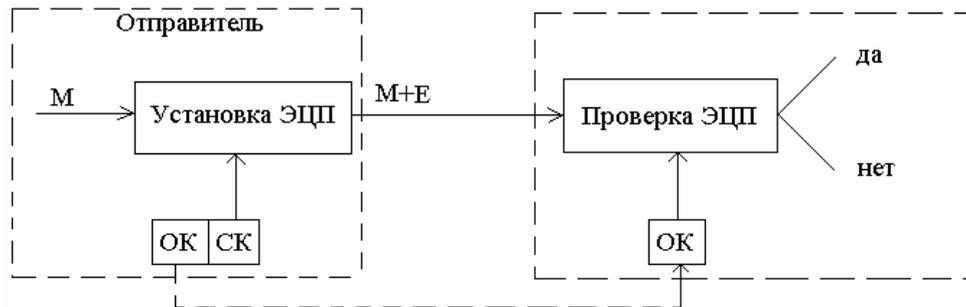


Рис. 2. Функциональная схема использования ЭЦП

Интерфейсы программы определения частоты символов представлены на рис.3., рис.4.

NN	DEC	HEX	CHAR	COUNT	%
1	32	20		347486	18,096
2	238	EE	о	161938	8,433
3	229	E5	е	113352	5,903
4	224	E0	а	113202	5,895
5	232	E8	и	95854	4,992
6	237	ED	н	89410	4,656
7	242	F2	т	81438	4,241
8	241	F1	с	74154	3,862
9	235	EВ	л	71458	3,721
10	240	F0	р	68334	3,559
11	226	E2	в	65558	3,466
12	234	EA	к	50450	2,627
13	228	E4	д	43304	2,255
14	236	EC	м	41834	2,179
15	239	EF	п	38912	2,026
16	243	F3	у	37808	1,974
17	44	2C	,	29452	1,534
18	251	FB	ы	29200	1,521
19	10	0A		29108	1,516
20	13	0D		29108	1,516
21	255	FF	я	26378	1,405
22	252	FC	ь	24904	1,297
23	227	E3	г	24310	1,266
24	46	2E	.	23582	1,228
25	231	E7	з	22730	1,184

Рис.3. Частота символов исходного текста

NN	DEC	HEX	CHAR	COUNT	%
1	126	7E	~	9166	0,477
2	84	54	T	8367	0,436
3	21	15	+	8275	0,431
4	45	2D	-	8235	0,429
5	255	FF	я	8151	0,424
6	32	20		8134	0,424
7	118	76	v	8101	0,422
8	48	30	D	8031	0,418
9	132	84	~	8028	0,418
10	250	FA	ь	8004	0,417
11	210	D2	T	7993	0,416
12	61	3D	=	7946	0,414
13	91	5B	l	7843	0,414
14	137	89	%	7826	0,413
15	54	36	б	7821	0,412
16	59	3A	:	7807	0,412
17	218	DA	ь	7804	0,412
18	161	A1	9	7855	0,409
19	11	08	~	7850	0,409
20	68	44	Z	7847	0,409
21	122	7A	z	7847	0,409
22	70	46	F	7845	0,409
23	195	87	±	7826	0,408
24	238	EE	о	7817	0,407
25	188	BC	j	7809	0,407
26	99	63	c	7793	0,406

Рис.4. Частотности символов зашифрованных текстов.



На основе анализа зашифрованных текстов мы можем сделать вывод, что частотности символов в них равномерно распределены в отличии от частотности исходного текста.

Скорость шифрования по алгоритму RSA является большей, чем скорость шифрования в других алгоритмах.

После изменения одного символа в файле «Orentext.txt» и после проверки истинности ЭЦП система не смогла распознать изменения.

В качестве организации криптографического обмена между двумя абонентами в симметричных и асимметричных криптосистемах были проделаны нижеперечисленные операции в нашей программе.

а. Зашифровали некоторый файл по симметричному алгоритму DES и вместе с ключом шифрования передали зашифрованный файл соседу.

б. Получили от соседа файл, зашифрованный по алгоритму DES, а также ключ шифрования, и попытались расшифровать данный файл.

с. Зашифровали для соседа некоторый файл по асимметричному алгоритму RSA и передали зашифрованный файл соседу.

д. Получили от соседа файл, зашифрованный по алгоритму RSA на Нашем открытом ключе, и попытались расшифровать данный файл.

Так как все операции прошли успешно, можно сказать, что получилось реализовать организацию криптографического обмена между двумя абонентами в симметричных и асимметричных криптосистемах.

### Литература

1. Теоретические основы компьютерной безопасности. Уч. Пособие для вузов по спец. "Компьютерная безопасность", "Компьютерное обеспечение информационной безопасности автоматизированных систем"/ П.Н. Девытин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербатов. – М.: Радио и связь.2000 – 190 с.

2. Основы информационной безопасности. Учебное пособие для вузов/Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов – М.: Горячая линия – Телеком, 2006-544 с.

3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001 – 368 с.

П.К. Шиверов, В.М. Пахомов

## ИСТОЧНИКИ ДОВЕРИЯ В КОНТЕКСТЕ СТОЙКОСТИ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ

(Самарский государственный университет)

### Введение

Анализ стойкости протоколов аутентификации, во многом, зависит от возможности установить наличие доверия между двумя или более общающимися абонентами сети.