

Постквантовые криптосистемы подписи и TLS-сертификаты

ФРСТ «Индата», МГТУ им. Н. Э. Баумана

Научный руководитель (ФРСТ «Индата»): Венедюхин А. А.

Авторы (МГТУ им. Н. Э. Баумана): Якубов П. Д., Проклашкина С. А.



Цель работы

- Утилита подписи файлов с помощью постквантовых алгоритмов цифровой подписи
- Утилита формирования TLS-сертификатов с постквантовой схемой цифровой подписи



Квантовый компьютер

- Оперирует кубитами в отличие от традиционных вычислителей с битами
- Способен решать некоторые задачи существенно быстрее, в их числе — выполнение алгоритма Шора
- Пока существенно “слабее” традиционных вычислителей, но количество используемых кубитов постоянно возрастает



Алгоритм Шора

- Алгоритм факторизации, позволяющий разложить большое число M на множители за разумное время
- Максимальное число, факторизованное на квантовом компьютере алгоритмом Шора — 35
- Теоретически может быть использован для взлома основных используемых на данный момент криптосистем



Постквантовый алгоритм

- Криптографический алгоритм, взломать который с помощью алгоритма Шора невозможно
- Примеры: ML-KEM (алгоритм инкапсуляции ключей), ML-DSA (алгоритм цифровой подписи)
- Постепенно встраиваются в существующие системы (доля ML-KEM в HTTPS составляет ~39% — данные с radar.cloudflare.com)



ML-DSA

- Module-Lattice-Based Digital Signature Algorithm
- Постквантовый алгоритм цифровой подписи
- Имеет 3 варианта с разной степенью защиты: ML-DSA-44, ML-DSA-65, ML-DSA-87
- В перспективе может заменить классические алгоритмы цифровой подписи: RSA, ECDSA
- Подписи сильно отличаются в размерах

Вариант	Размер в байтах		
	Секретный ключ	Открытый ключ	ЭП
ML-DSA-44	2560	1312	2420
ML-DSA-65	4032	1952	3309
ML-DSA-87	4896	2592	4627



Особенности использования ML-DSA

- Существуют библиотеки для Golang, C, Rust, Python, Java, JS
- Комбинируют с ECDSA для сочетания постквантовой и классической защиты
- Сравнительная таблица скорости работы различных алгоритмов:

=====				
Algorithm	Level	KeyGen	Sign	Verify

ML-DSA	44	84μs	212μs	36μs
ML-DSA	65	150μs	339μs	50μs
ML-DSA	87	220μs	373μs	72μs
ECDSA	P384	108μs	171μs	499μs
RSA	3072	156.256ms	909μs	31μs



Результаты работы

Использован язык Go с библиотеками `cloudflare/circl` для ML-DSA и `crypto` для остальных криптосистем

Утилита подписи файлов

- Реализация всех сценариев работы — генерация ключей, подпись файлов, проверка
- Передача ключей происходит в формате PEM
- Присутствует композитный режим работы — ML-DSA + ECDSA



Результаты работы

Утилита генерации сертификатов

- В набор функций стандартной библиотеки языка Go добавлена поддержка ML-DSA-65
- Позволяет генерировать TLS-сертификаты с подписями типа ML-DSA-65

```
1 Certificate:
2   Data:
3     Version: 3 (0x2)
4     Serial Number:
5       7f:43:c0:4e:96:47:ed:e6:f8:e1:18:2e:08:21:73:66:ed:a9:b0:43
6     Signature Algorithm: 2.16.840.1.101.3.4.3
7     Issuer: O=CA_ORG
8     Validity
9       Not Before: Jan  1 00:00:00 2025 GMT
10      Not After : Jan  1 00:00:00 2026 GMT
11     Subject: O=ORG
12     Subject Public Key Info:
13       Public Key Algorithm: 2.16.840.1.101.3.4.3
14       [... ML-DSA-65 Public key ...]
15     X509v3 extensions:
16       X509v3 Key Usage: critical
17         Digital Signature
18       X509v3 Extended Key Usage:
19         TLS Web Server Authentication
20       X509v3 Basic Constraints: critical
21         CA:FALSE
22       X509v3 Authority Key Identifier:
23         keyid:03:23:ED:79:96:30:A7:30:CA:2E:CB:76:6C:A2:25:52:CC:E1:DD:F6
24       X509v3 Subject Alternative Name:
25         DNS:tldcon.ru
26     Signature Algorithm: 2.16.840.1.101.3.4.3
27     [... ML-DSA-65 Signature ...]
```



Возможные проблемы

- Трафик в любых инфраструктурах с открытым ключом (PKI) существенно увеличится
- TLS: превышает размер TLS-записи, начинается фрагментация (IPv4)
- DPI: нужна поддержка фрагментированных записей



Возможные проблемы: DNSSEC

- Ключи не помещаются в стандартный размер DNS-пакета (включая EDNS)
- Замена типа ключей потребует изменений по всей цепочке (замена корневого ключа вызовет проблемы)
- Неготовность DNS-операторов внедрять новые технологии

ECDSA (P-256) vs ML-DSA-65

1 30:a5:89:4d:57:81:f2:ea:86:83:66:f6:16:5e:20:32:42:24:6e:
2 02:20:3f:d7:1a:e5:64:0e:85:18:eb:f6:c5:cb:37:72:7a:23:
3 a0:13:10:c0:14:71:e9:62:6a:52:f3:5f:fd:9f:a0:5b
4

1	1e:67:21:81:5d:64:22:5a:54:a5:88:ad:50:9c:fd:c0:fa:8b:	41	f1:a3:32:c6:93:49:94:9c:f1:64:23:fb:9f:b4:3a:e0:14:70:	81	7a:95:29:d7:c0:0a:e7:73:b3:ae:0a:2f:ad:a7:01:ad:89:0a:47:	121	42:2a:63:18:f5:05:28:2f:a4:28:6c:dc:d2:d9:78:d2:d9:	161	1c:25:ac:a0:01:f0:71:65:e7:dc:60:2a:e6:f6:b6:80:11:a8:d4:
2	57:4d:c1:8f:0a:f0:49:e9:7d:79:03:0a:ec:6f:2d:f8:07:5b:	42	98:c6:32:b5:47:ec:82:f5:18:0d:57:65:f2:02:f6:6b:5b:c1:	82	81:c4:f4:e4:8a:88:95:ed:e0:99:86:ee:53:83:95:aa:c2:f:	122	97:c3:12:52:a5:8e:9c:a6:f4:f5:ea:d3:67:97:7a:40:98:35:	162	75:8f:9e:77:0e:ea:e7:29:0e:4e:85:0b:1f:14:34:ba:f6:59:
3	74:92:50:74:1a:70:43:5d:ee:cd:f1:1e:17:3e:7b:dd:89:76:	43	1d:a4:64:96:57:66:67:fa:e4:5e:6b:92:10:18:e9:9f:35:ff:01:	83	18:f1:f8:fe:7a:3b:07:e8:d2:41:8a:ea:50:8a:cc:63:ae:70:	123	ad:b7:f4:a5:94:1d:68:6a:83:02:d5:88:a7:69:02:73:22:46:	163	7b:f7:d6:46:23:66:c4:0a:91:63:1f:b0:37:9f:ab:57:43:36:
4	f4:b1:e2:88:b1:a9:0d:54:c0:8a:79:b2:5a:5e:2d:14:03:	44	b5:c4:bf:c1:60:e6:85:45:01:15:0f:00:0a:95:7c:f1:16:7b:	84	d3:65:bf:c4:21:02:2b:5b:04:34:e8:bb:f5:cc:bf:6b:5e:4a:	124	fe:b0:4f:ad:0a:60:f6:ee:8c:3c:d8:f4:01:47:b6:85:7f:99:	164	b0:cd:c4:1f:43:45:0c:70:e8:57:aa:c4:54:0e:3f:9f:f4:7f:
5	6f:18:8e:87:22:20:3f:db:5f:d1:1a:c8:5f:7d:3a:d1:86:77:	45	50:87:13:8a:0a:1a:ad:ce:06:61:c3:2c:02:f9:c9:b6:6d:5f:	85	ef:7e:42:ce:13:5a:00:19:f7:b6:63:dd:77:c1:23:af:5a:ed:	125	94:e3:7a:3a:9c:27:f3:0e:b8:32:c7:49:86:6f:9c:7:cea:61:	165	4c:9f:9c:53:1e:0f:4e:00:d5:06:90:11:ac:c4:b4:b6:05:3d:
6	6e:c1:8e:90:8c:7a:4b:28:51:7c:98:1a:0e:6d:30:a5:e2:22:30:	46	33:34:b7:ab:34:53:2f:35:45:7b:25:31:33:a8:cc:5f:7b:3a:	86	58:3f:da:7f:5d:0b:b3:b7:07:57:6e:5e:3a:99:47:b3:e7:71:	126	7f:6e:7c:5c:69:3e:79:84:f6:bfc:ec:a4:13:45:73:9a:df:b0:	166	20:dd:c8:bf:94:49:21:77:87:10:75:5e:29:b9:b9:be:d9:b6:c7:
7	27:0d:28:63:d2:56:b0:6e:c7:f0:ea:1f:ef:77:7a:c3:37:75:	47	9a:7f:0f:98:68:b4:12:4f:df:d8:6a:9a:88:25:21:d1:80:18:	87	fb:13:27:6e:7e:7c:81:0d:a3:fcc:21:ac:f0:aa:8e:de:7e:	127	d1:67:03:54:54:ff:12:0d:64:c3:d8:af:16:d7:dd:37:d3:02:	167	cb:c3:51:45:6e:51:db:3c:53:f7:1f:3e:70:96:f2:8a:00:3c:
8	f3:ed:e9:85:27:d9:1d:46:c1:d4:f2:b1:31:e4:0e:0e:77:	48	74:8a:72:2c:a3:55:68:df:72:5e:7a:dd:9e:d3:1f:53:55:a1:	88	9c:39:60:53:31:40:eb:ac:6a:2a:1f:5f:a4:4a:23:f4:b1:66:	128	02:e7:f2:69:65:6e:c0:7c:97:d3:2a:ec:b2:a6:ee:89:b0:e9:	168	a1:e0:b2:b5:55:0e:55:38:57:da:de:aa:31:2f:ed:43:a3:13:
9	2b:7b:37:ec:23:24:6c:12:fbc:cc:00:22:52:9e:ac:af:79:24:	49	6c:a5:ff:7e:9e:2d:30:07:da:b6:b9:b0:cd:f2:e1:a6:e1:7d:	89	6b:0f:9c:ed:c4:23:45:f5:b6:a0:44:b9:69:bd:7a:da:0e:	129	46:28:c7:64:65:45:f7:3c:28:eb:a6:44:42:b1:1e:29:26:de:	169	40:34:27:78:3d:0b:b2:6d:32:e7:38:c4:c1:7a:cf:d2:6b:a1:
10	f8:f6:31:32:c8:ee:aed:f1:bb:96:33:55:dd:fc:98:4c:9b:b6:	50	13:99:08:0e:7a:20:7a:16:16:e4:2e:d3:16:c5:5d:00:6f:78:	90	99:2d:7b:9a:75:85:63:c1:6f:9d:c0:a2:5b:c7:c1:5b:0b:0a:	130	e2:85:75:4f:06:0d:c3:73:ed:49:06:e1:77:c6:68:03:05:de:	170	71:93:07:78:09:a6:c0:4d:c2:b3:25:ba:70:2d:25:45:7d:42:
11	bb:7f:96:ab:e2:3b:f6:c1:7d:50:07:da:06:3e:3c:f8:30:a9:	51	4d:46:0e:59:50:09:5c:06:f6:5a:ed:dd:eb:d1:b4:92:39:09:	91	40:c2:1d:77:38:eb:27:6e:61:07:32:a7:22:cb:cd:2a:9a:1b:	131	88:7a:95:07:90:79:53:30:f5:b0:b0:b9:f3:ee:89:55:df:3c:	171	ac:87:02:b8:41:f2:af:cccc:9e:06:a9:c6:99:ef:48:98:06:
12	e1:6f:9f:52:d6:f4:cb:14:4f:05:93:93:b0:04:47:54:e6:dd:	52	4b:22:1d:81:04:c3:c6:f6:9a:0b:dd:27:b5:98:fb:be:f0:0e:	92	3f:a3:6f:1d:7f:58:6f:92:89:0c:d2:56:a1:e8:ac:da:3a:95:	132	71:c4:fff:1e:c4:42:20:c7:7a:b0:3c:4c:e5:f1:fe:ad:85:18:	172	e4:c3:c5:9e:93:71:a4:85:fe:3d:a6:e0:1e:01:f4:d6:b5:52:
13	0f:64:2b:15:14:66:49:71:ce:e7:c2:67:8a:c3:0a:8d:68:5d:56:	53	fcc:ec:9c:63:3a:e5:22:02:5b:0e:a9:c1:fc:58:05:27:55:31:	93	35:f0:7d:85:93:56:76:f7:5f:5c:91:8c:1e:21:bc:5b:c8:56:78:	133	bl:9c:bac:0a:80:7a:19:b2:96:79:12:97:5a:a1:99:b3:e2:e7:	173	1b:29:cb:d2:16:1d:d6:2c:66:5e:81:b2:77:00:27:eb:4b:cf:
14	b7:da:61:5f:14:d6:63:08:68:3d:24:67:45:93:14:7a:14:95:	54	0b:3f:da:83:94:ce:e4:04:35:99:89:b6:3c:6f:70:3a:4c:38:7f:	94	80:cc:92:7e:1c:bl:b2:b4:e6:a3:df:dc:41:bb:c2:9a:78:0f:	134	37:c5:d1:ef:8c:09:14:f1:28:a5:1a:39:c2:e9:5b:a9:1c:3e:	174	a6:0d:3f:7c:7c:88:33:74:4c:7d:05:c0:ee:ec:22:d2:7d:
15	fa:fe:98:b4:ba:4b:53:00:8f:59:6b:45:9d:c3:24:cd:29:70:	55	92:10:90:b8:ea:8d:63:0e:0f:b5:09:46:18:29:b0:60:54:9c:	95	14:e5:93:ad:bd:ff:73:81:c4:9a:12:c8:50:85:ad:ce:b8:c5:	135	4fa:77:c7:65:6f:13:9f:f6:67:cf:91:19:e8:27:9c:eb:cf:78:	175	4b:c1:bd:1f:6b:9e:ed:36:d0:24:3bc:6a:c0:3c:f5:0f:4e:
16	73:bf:42:8d:1f:81:15:39:99:7a:71:6d:63:ba:93:45:1a:19:	56	87:6d:13:23:07:81:f8:94:85:64:39:a9:b9:6d:60:8d:9b:	96	f1:54:e5:54:82:9b:c3:ba:a5:f0:60:9b:ae:42:10:21:a3:7b:	136	78:a6:8a:78:04:39:93:3a:13:3bc:31:d9:1b:6f:11:2e:bf:67:5c:	176	84:5f:bd:11:6b:8b:54:0a:33:05:5d:d4:f3:08:c0:2e:f5:97:
17	f1:63:64:8a:c6:26:3a:1b:1e:f4:28:21:d5:75:17:59:2e:b6:	57	fbc:cc:a0:b9:15:94:09:ff:98:80:b7:f5:c9:46:1a:29:87:	97	20:72:f0:a8:4d:27:80:1e:a1:a7:93:7e:d1:d3:ec:d5:10:3f:	137	77:53:ec:a3:c3:d5:ce:12:d5:9c:1a:9c:fe:89:2a:12:06:24:7d:	177	68:c0:bd:11:8b:28:a4:72:f5:72:f6:4e:b2:6a:6d:4e:b0:01:
18	8d:06:58:10:66:52:85:0b:99:02:98:45:a0:46:35:c8:34:cf:	58	72:08:07:11:fb:1c:6d:82:c5:de:89:9c:02:7f:70:72:71:35:	98	39:49:78:a6:34:fc:4c:f1:91:09:b9:76:1a:1b:b0:d4:f4:17:be:	138	76:a8:ad:3a:6b:c2:18:28:8c:b9:58:fd:76:8e:77:bb:f6:1b:	178	31:c9:97:1b:18:85:f5:3c:81:0a:30:fb:5a:cd:ff:d9:dc:e7:
19	ef:3a:1d:0d:3a:82:34:82:34:82:34:82:34:82:34:82:34:82:	59	e1:51:bc:d2:89:0c:29:5b:a3:79:f5:ba:9c:f4:19:20:14:91:2e:	99	cb:0d:0e:77:0b:2a:3e:9a:2d:03:83:54:0e:03:c5:1a:7b:	139	2ba:f:b4:54:d3:dc:b2:7f:6b:0a:8a:06:23:9f:99:ef:71:d5:	179	4e:48:c5:b6:16:31:8d:02:96:f3:b5:5e:5a:2e:1b:c3:c6:
20	e2:a2:d2:8a:03:12:f1:91:6a:1c:3c:b2:d5:05:03:fe:79:04:	60	46:03:93:19:2d:02:04:c5:9c:08:ce:3d:3f:78:5a:33:d1:66:	100	7a:7b:12:58:4a:00:02:17:f1:4b:a7:7c:fa:6e:7f:05:57:67:48:	140	e5:40:3e:7d:63:4e:8a:e5:0b:01:63:65:57:e7:4d:07:90:54:	180	62:67:99:9e:3c:1e:51:0e:2e:2a:cd:f0:1f:54:9d:b9:67:
21	53:b0:bb:c2:aed:8a:7a:83:af:bf:66:4a:02:04:ed:c7:6a:52:0e:	61	22:d9:22:64:53:4f:d4:34:6f:ff:f4:df:26:a6:d1:a2:37:13:	101	b7:37:27:fe:0f:a8:34:2a:67:07:8a:8b:f0:0f:02:32:02:b7:	141	66:61:0e:3f:ea:a2:b8:f0:78:64:3f:11:8b:46:43:01:da:32:	181	77:98:0e:31:5b:9c:9e:bd:cf:f2:ff:05:09:1d:31:4f:8f:
22	b9:8a:de:f9:48:7a:7a:03:c1:67:cd:bb:8a:73:6f:b0:1f:	62	64:3d:cc:c1:d0:07:97:35:95:8f:03:cd:0e:cf:d9:2f:54:03:	102	99:6e:fc:c3:5b:cd:23:68:1d:e7:8a:02:9f:78:0a:05:f3:ec:	142	1f:6f:b1:0c:24:30:1a:9d:27:6c:c0:24:33:4c:66:7c:28:ad:	182	90:99:14:45:00:70:7a:94:a0:00:00:00:00:00:00:00:00:
23	c4:0d:5d:1b:32:14:4e:7e:9a:0d:7f:09:68:37:a9:7a:a5:0f:	63	6d:4e:ef:98:13:b8:4a:78:c2:9a:db:e1:6c:3d:ed:c1:52:f4:61:	103	30:69:b9:58:5b:3a:70:b1:52:68:18:78:03:3d:b7:e7:	143	58:14:d9:25:63:40:b9:83:92:73:66:9c:7c:dc:eb:6f:7e:30:	183	00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
24	77:9d:94:5f:52:d1:51:53:7a:76:16:ec:0e:45:84:1a:16:	64	73:23:2e:e7:a7:1d:a3:ec:7d:7a:07:86:5a:ac:14:47:f6:ed:	104	ef:8e:04:24:6c:5d:40:0a:f4:12:27:3c:67:a5:bb:1b:c9:74:c7:	144	21:3d:94:e6:4b:25:05:da:7b:ec:37:be:7f:7a:76:7f:f0:17:3:	184	
25	d5:95:f0:6e:cf:f9:b0:6b:38:bd:76:22:4d:f4:d6:9b:05:1:	65	98:b2:9e:0c:83:ed:89:48:82:91:f5:9f:8c:b3:96:8c:be:47:	105	cb:6e:04:64:2d:5d:00:9a:f1:22:39:89:39:dd:db:ff:f7:87:	145	27:ed:89:41:17:97:c7:3f:4e:a4:9e:0b:79:67:55:7c:41:72:		
26	71:47:08:3c:83:c9:b9:b6:b1:f47:el:d0:22:ea:8d:c4:14:4e:ad:	66	90:2d:5d:70:93:80:0e:8b:0e:84:40:39:1a:a6:06:07:b3:22:	106	45:a5:85:77:ce:88:3e:22:3a:72:c6:9a:1a:df:22:32:c1:7b:	146	b8:a5:01:66:c6:09:1e:25:09:4e:24:1b:b8:34:25:f1:57:c7:		
27	51:47:c3:83:c9:b9:b6:b1:f47:el:d0:22:ea:8d:c4:14:4e:ad:	67	7a:43:96:71:2e:40:b8:ca:5a:cc:75:d5:ec:07:ff:55:4a:08:	107	20:44:41:01:bc:0b:8c:70:38:10:31:67:05:85:f7:73:40:	147	aa:12:8a:0b:4d:f3:c1:6b:ab:11:a1:a6:68:42:27:53:76:80:		
28	00:55:8e:9d:32:8a:cb:0b:e2:3c:a3:32:6c:83:52:75:d7:a1:	68	10:75:c6:9a:7c:d4:30:08:18:5c:df:70:7b:09:52:4d:43:33:	108	3e:aa:f4:aca:05:c0:27:95:6f:02:87:7b:97:3f:1a:5a:b5:ec:	148	3f:b0:6e:6f:6d:0e:42:76:94:a8:66:b6:2d:40:4a:06:13:07:		
29	06:80:b0:aa:b5:f3:44:59:6f:72:2f:3a:db:94:6f:6a:76:	69	78:09:03:b8:00:90:00:06:43:42:72:dd:81:0e:7f:56:63:	109	03:9f:49:f2:8e:84:bl:56:08:02:5f:82:6f:47:98:b7:0a:	149	cl:15:16:05:4e:1f:92:ed:42:8c:7e:94:43:43:09:03:52:27:		
30	4e:9a:cd:02:03:6f:45:c6:08:8a:b7:26:67:29:0e:1f:46:0a:25:	70	63:7d:44:7a:70:b7:7c:2a:7b:7c:2a:13:4a:c1:0e:44:	110	aed:cb:bf:0c:ad:7f:0d:1f:0e:02:4c:35:3e:4a:5f:c4:f0:48:	150	25:1a:5a:6b:b9:0d:f0:02:d2:21:72:d9:84:53:b5:48:0e:4f:12:		
31	3f:00:50:21:9a:6e:76:75:fa:5a:0b:7d:24:00:63:68:92:fd:	71	e8:4c:57:e5:d2:c5:a9:16:7d:71:71:64:00:b0:52:98:97:	111	50:73:98:43:0a:54:2a:b5:84:60:f1:93:49:11:dc:0a:02:ff:	151	94:ac:bb:05:d9:13:20:00:20:c7:23:1a:34:09:c4:0e:91:41:		
32	47:16:de:06:bab:95:f9:99:c6:44:97:9a:9c:37:35:fe:a0:4:	72	21:a2:ed:52:4d:6c:e8:18:cd:42:dd:5c:f7:b4:36:1f:8f:65:	112	6e:3e:12:e7:53:0c:5a:6b:00:1c:a9:02:0c:ab:74:7d:ae:f3:	152	71:ef:de:ad:ae:b6:a0:01:6b:b5:4e:20:ad:af:56:08:17:		
33	89:0c:58:f5:10:77:24:86:2d:ebd:9e:f9:3a:53:5d:03:	73	45:16:cf:21:75:6d:11:0d:7a:74:53:05:51:2b:1b:0a:8f:	113	0b:7b:48:0c:4a:7e:4d:68:53:0b:2c:55:02:92:c1:22:09:27:	153	1f:72:6a:0b:92:3c:36:a2:ed:68:03:eb:fa:64:9e:c0:b0:b3:		
34	e9:04:43:41:22:22:0c:32:88:42:b2:136:f47:9a:53:24:90:	74	aec:3d:00:ac:b4:cb:4b:7d:74:53:14:55:b6:96:b0:ad:8f:1b:	114	8f:3b:bd:ea:20:4d:bb:3a:22:99:0b:ff:69:9c:5a:f5:44:	154	41:72:a6:19:29:3c:36:a2:ed:68:03:eb:fa:64:9e:c0:b0:b3:		
35	ec:d5:fd:4a:7e:5d:59:38:b7:e6:a5:16:3d:09:ee:a3:c9:ca:	75	cc:22:84:ea:af:97:7c:19:0f:8f:5c:37:32:41:ac:c5:78:eb:	115	7a:10:77:e9:06:3b:08:0e:62:1a:3c:0a:b9:bc:84:20:b5:1d:	155	73:5f:8e:1e:7b:85:05:57:34:68:9b:5d:8b:08:30:4f:4e:94:		
36	67:88:9d:42:9e:a2:46:c6:4e:9c:83:c7:81:6c:5f:59:5e:76:	76	d5:06:a0:18:e4:6d:4b:bb:52:c6:00:48:da:32:3c:07:07:6a:	116	3a:1a:08:07:b5:22:49:0b:06:a5:08:9a:08:28:3b:77:1f:	156	79:98:5c:4f:c0:1a:bl:db:51:52:87:c6:51:99:50:ad:90:62:		
37	87:22:67:7d:7c:9e:7e:8a:0a:31:bd:a3:24:9f:1d:27:2f:	77	78:09:af:9f:0c:47:ae:7c:35:9c:06:9e:0c:10:0b:9b:1c:c3:	117	42:32:48:93:78:0a:6a:06:6c:f3:34:81:fa:eb:af:87:68:	157	18:36:43:04:d7:52:7f:4a:3a:6e:57:f8:0a:72:1a:dc:01:1b:		
38	9c1:4a:fb:c1:d1:a6:a5:42:14:74:2f:85:3d:b1:a5:42:78:	78	2c:a2:e1:8c:b6:2a:11:02:03:75:05:f4:5a:24:8c:a8:08:95:	118	5d:93:94:f4:8b:b7:10:1e:94:af:08:18:b8:7b:1f:6b:8:08:	158	fa:69:0e:ec:21:a6:05:01:2b:85:8d:0c:7d:9a:bf:ed:88:		
39	f9:91:7d:4a:6d:fd:42:6d:17:43:f2f:86:67:be:f3:33:40:	79	24:2a:24:1a:67:ba:10:a6:2a:ce:ce:83:80:ed:fb:9d:5d:6f:	119	3e:b3:2e:47:c2:35:c4:e6:43:7f:21:58:b3:7a:f1:53:78:c2:	159	c5:51:8e:01:c8:01:29:1d:55:54:c8:18:0d:3a:52:5c:bf:c4:		
40	a2:d9:37:cd:03:20:8a:7a:c9:67:77:92:89:ff:df:2a:54:7d:	80		120		160	b0:56:7a:81:b2:ca:75:5d:bd:66:c3:9d:36:b5:13:81:40:07:		

Спасибо за внимание!