ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(РОССТАНДАРТ)

Технический комитет 026

«Криптографическая защита информации»

СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ

ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

ПО ИСПОЛЬЗОВАНИЮ ГОСТ 28147-89 ПРИ ШИФРОВАНИИ ВЛОЖЕНИЙ В ПРОТОКОЛЕ IPSEC ESP

Утверждена решением заседания
технического комитета по стандартизации
«Криптографическая защита информации»
(Протокол №12 от 21.11.2013 г.)

Москва
2013

Содержание

1 Введение

Протокол инкапсуляции зашифрованных данных (Encapsulating Security Payload, ESP) используется для обеспечения конфиденциальности, целостности и аутентичности содержимого IP-пакетов и входит в группу протоколов защиты сетевого трафика на IP-уровне – IP Security (IPsec). Полное описание протокола ESP приведено в документе **RFC4303**.

Данный документ содержит описание использования алгоритма ГОСТ 28147-89 при шифровании вложений IPsec ESP, но она не определяет криптографический алгоритм ГОСТ 28147-89 и форматы представления криптографических типов данных.

В данном документе алгоритм и представление данных определены требованиями национального стандарта ГОСТ 28147-89, а представление параметров соответствует определенному в документах **RFC4357** и **RFC4490**.

В данном документе определяются следующие преобразования вложений в рамках протокола ESP:

- комбинированное преобразование ESP_GOST-4M-IMIT;
- комбинированное преобразование ESP_GOST-1K-IMIT.

ESP-вложения обрабатываются в рамках IPsec SA, параметры которой МОГУТ быть интерпретированы согласно положениям, определенным в документе **RFC2407**.

Необходимость разработки данного документа вызвана потребностью в обеспечении совместимости реализаций протоколов IPsec российских производителей.

2 Нормативные ссылки

Указанные в этом разделе рекомендаций ссылочные документы являются обязательными для их применения. Для датированных ссылок используют только указанное здесь издание. Для недатированных ссылок — последнее и актуальное издание со всеми изменениями и дополнениями:

ГОСТ 28147-89 — Государственный комитет СССР по стандартам, «Защита криптографическая. Алгоритм криптографического преобразования», Государственный стандарт СССР, ГОСТ 28147-89, 1989.

ТК26IKE — Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 в протоколах обмена ключами IKE и ISAKMP», 2013.

ТК26АН — Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию алгоритмов обеспечения целостности IPsec (AH, ESP) на основе ГОСТ Р 34.11-94», 2013.

2.1 Дополнительные ссылки

RFC2119 — С. Браднер, «Ключевые слова для использования в документах RFC, указывающие уровень требований», стандарт BCP 14, март 1997 г. (Bradner S., Key words for use in RFCs to Indicate Requirement Levels, BCP 14, IETF RFC 2119, March 1997).

RFC2407 — Д. Пайпер, «Область интерпретации IPsec для ISAKMP» (Piper D., The Internet IP Security Domain of Interpretation for ISAKMP, IETF RFC 2407, November 1998).

RFC4301 — С. Кент, К. Сео, «Архитектура безопасности для протокола IP» (Kent S. and K. Seo, Security Architecture for the Internet Protocol, IETF RFC 4301, December 2005).

RFC4303 — С. Кент, «Инкапсуляция защищенных данных IP (ESP)» (Kent S., IP Encapsulating Security Payload (ESP), IETF RFC 4303, December 2005).

RFC4304 — С. Кент, «Добавление расширенных порядковых номеров (ESN) в области интерпретации IPsec (DOI) для протокола управления защитными связями и ключами (ISAKMP)» (Kent, S., Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP), IETF RFC 4304, December 2005).

RFC4357 — В. Попов, И. Курепкин, С. Леонтьев, «Дополнительные алгоритмы шифрования для использования с алгоритмами по ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94» (Popov V., Kurepkin I. and S. Leontiev, Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms, IETF RFC 4357, January 2006).

RFC5116 — Д. Макгрейв, «Интерфейс и алгоритмы для аутентификации при шифровании» (McGrew D., An Interface and Algorithms for Authenticated Encryption, IETF RFC 5116, January 2008).

RFC5282 — Д. Блэк, Д. Макгрейв, «Использование аутентификационных алгоритмов шифрования с зашифрованными вложениями протокола IKEv2 (Internet Key Exchange, версия 2)» Black, D. and D. McGrew, Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol, IETF RFC 5282, August 2008.

RFC5996 — С. Кауфман, П. Хофман, Й. Нир, П. Еронен, «Протокол обмена ключами в сети Интернет, версия 2 (IKEv2)» (Kaufman C., Hoffman P., Nir Y., and P. Eronen, Internet Key Exchange Protocol Version 2 (IKEv2), IETF RFC 5996, September 2010).

RFC6311 — Р. Сингх, Г. Кальяни, Ю. Нир, Ю. Шеффер, Д. Чжан «Протокольная поддержка высокой доступности IKEv2/IPsec» (Singh R., Kalyani G., Nir Y., Sheffer Y. and D. Zhang, Protocol Support for High Availability of IKEv2/IPsec, IETF RFC 6311, July 2011).

2.2 Информативные ссылки

ГОСТ Р 34.11-94 — Государственный комитет Российской Федерации по стандартам, «Информационные технологии. Криптографическая защита информации. Функция хэширования», ГОСТ Р 34.11-94, Государственный стандарт Российской Федерации, 1994.

ГОСТ Р ИСО/МЭК 7498-1-99 — Государственный комитет Российской Федерации по стандартам, «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель», (Information technology. Open systems interconnection. Basic reference model. Part 1. The basic model), ИПК Издательство стандартов, 1999.

ПП РФ №313 — Постановление Правительства Российской Федерации от 16 преля 2012 г. № 313 «Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

RFC2409 — Д. Харкинс, Д. Каррел, «Протокол защищённого согласования и аутентичности доставки идентифицированного материала для сопоставления безопасности (IKE)» (Harkins, D. and D. Carrel, The Internet Key Exchange (IKE), IETF RFC 2409, November 1998).

RFC2675 — Д. Борман, С. Диринг, Р. Хинден, «Слонограммы IPv6» (Borman, D., Deering, S., and R. Hinden, IPv6 Jumbograms, IETF RFC 2675, August 1999).

RFC4490 — С. Леонтьев, Г. Чудов, «Методические рекомендации по использованию алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001 с синтаксисом криптографических сообщений (CMS)» (S. Leontiev, G. Chudov, Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS), IETF RFC 4490, May 2006).

RFC4491 — С. Леонтьев, Д. Шефановский, «Методические рекомендации по использованию алгоритмов ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94 в профиле сертификата и списка отзыва сертификатов инфраструктуры открытых ключей X.509 Интернет» (S. Leontiev, D. Shefanovski, Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF RFC 4491, May 2006).

RFC6071 — С. Френкель, С. Кришнан, «Дорожная карта для протоколов IP Security (IPsec) и Internet Key Exchange (IKE) в документах» Frankel, S. and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", IETF RFC 6071, February 2011.

Примечание: При пользовании данным документом целесообразно проверить действие ссылочных стандартов и классификаторов в информационной системе общего пользования - на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании данным документом следует руководствоваться замененным (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Основные понятия, термины и определения

В документе используются термины и определения стандартов IPsec (**RFC4301**) и ESP (**RFC4303**), далее приводятся только дополнительные определения.

3.1 Терминология требований

Термины "ДОЛЖНО", "ДОЛЖНА", "ДОЛЖНЫ", "ДОЛЖЕН" (MUST, REQUIRED, SHALL), "НЕ ДОЛЖЕН", "НЕ ДОЛЖНЫ" (MUST NOT, SHALL NOT), "РЕКОМЕНДУЕТСЯ" (SHOULD, RECOMMENDED), "НЕ РЕКОМЕНДУЕТСЯ" (SHOULD NOT, NOT RECOMMENDED), "МОГУТ", "МОЖЕТ" (MAY, OPTIONAL) в рамках этого документа ДОЛЖНЫ интерпретироваться в соответствии с положениями документа **RFC2119**

3.2 Определения

В данном документе определены следующие термины:

IKE (Internet Key Exchange)	протокол защищенного согласования ключей, используется для формирования сопоставлений безопасности (SA);
IPsec (сокращение от IP Security)	набор протоколов по обеспечению защиты данных, передаваемых по межсетевому протоколу IP, включает в себя протоколы согласования ключей и защиты сетевого трафика;
Гаммирование	процесс наложения по определенному закону гаммы шифра на открытые данные;
Имитовставка	отрезок информации фиксированной длины, полученной по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты;
Имитозащита	защита системы шифрованной связи от навязывания ложных данных;
Искажённый пакет	ESP-вложение, для которого вычисленное значение ICV не совпало с переданным значением;
Пакет с искажённым Seq#:	ESP-вложение, для которого не прошёл предварительный контроль соответствия SPI и *Seq#* или не совпала старшая часть ICV для ESP_GOST-1K-IMIT;
Сопоставление безопасности (Security Association, SA)	совокупность атрибутов безопасности и ключевой информации, ассоциируемая с безопасным соединением, представляющим собой виртуальный однонаправленный канал для передачи данных;

Хэш-функция (функция хэширования)	функция отображения последовательности байт в последовательность байт фиксированного размера;

3.3 Условные обозначения

В данном документе используются следующие обозначения:

encryptCNT (IV, K, D)	шифрование ГОСТ 28147-89 в режиме гаммирования на ключе K данных D с начальным вектором IV;
decryptCNT (IV, K, D)	расшифрование ГОСТ 28147-89 в режиме гаммирования на ключе K данных D с начальным вектором IV;
Divers (K, D)	алгоритм диверсификации ключа K по данным диверсификации D (раздел 7 **RFC4357**, узел замены выбирается согласно параметрам раздела 6.1 настоящего документа, в рамках данного документа в качестве данных диверсификации передаётся последовательность 8 байт, содержащая 64-битное целое число в сетевом порядке байт);
gost28147IMIT (IV, K, D)	выработка имитовставки ГОСТ 28147-89 на ключе K от данных D, с внутренним выравниванием нулями до границы блока 8 байт;
A	ассоциированные данные (AEAD в **RFC5116**, по ГОСТ могут содержать адресную часть, отметку времени, синхропосылку и др.);
Seq#	64-битный номер пакета (если ESN из **RFC4304** не согласован, то значение Seq# всегда принадлежит диапазону 1.. 2^32-1;
Seq#h	старшая часть Seq#;
Seq#l	младшая часть Seq#;
IV (Seq#)	синхропосылка пакета Seq#;
Kc_e (Seq#)	ключ комбинированного алгоритма шифрования пакета Seq#;
Kc_i (Seq#)	ключ комбинированного алгоритма имитозащиты пакета Seq#;
Kc_i2 (Seq#)	ключ предварительного контроля пакета Seq# (только для ESP_GOST-1K-IMIT);

Kr_e	корневой ключ шифрования SA;
Kr_i	корневой ключ имитозащиты SA;
KeyMeshing	алгоритм усложнения ключа, описанный в **RFC4357**;
SPI-Auth-Code	код аутентификации, вычисляемый в рамках ISAKMP SA (протокола CPIKE или другого протокола согласования ключей) для данной IPsec SA, предназначенный для аудита событий и предварительного контроля пакета;
substr (s..f, bytes)	последовательность байт с байта s, по байт f, выбранная из последовательности bytes, представленной в сетевом порядке байт;

3.4 Аббревиатуры и сокращения

В тексте данного документа используются следующие сокращения и аббревиатуры:

ESN	расширенный номер пакета (Extended Sequence Number, **RFC4304**);
ISAKMP	протокол управления ключами и группами атрибутов сетевой безопасности (Internet Security Association and Key Management Protocol);
MTU	максимальный размер данных, который может быть единовременно передан на канальном уровне сетевой модели OSI в соответствии с ГОСТ Р ИСО/МЭК 7498-1-99 (Maximum Transmission Unit);

4 Состав сопоставления безопасности ESP SA

Протокол ISAKMP предоставляет механизмы согласования атрибутов безопасности. Базовое описание протокола ISAKMP содержится в документе **RFC2408**.

В рамках ISAKMP SA (протокола CPIKE или другого протокола согласования ключей) для данной IPsec SA, как минимум, согласуются следующие компоненты:

- 32-битный код аутентификации SPI (неконфиденциален);
- 256-битный симметричный ключ *Kr_e*;
- 256-битный симметричный ключ *Kr_i*;
- параметры ГОСТ 28147-89;
- максимальный объём данных сопоставления безопасности (Lifetime SA, Kbytes);
- максимальное время жизни SA (Lifetime SA, sec);
- максимальное значение счётчика искажённых пакетов.

В зависимости от преобразования размеры согласуемого ключевого материала (KEYMAT) следующие:

- для ESP_GOST-4M-IMIT — 36 байт (*Kr_e* и *SPI-Auth-Code*);
- для ESP_GOST-1K-IMIT — 68 байт (*Kr_e, Kr_i* и *SPI-Auth-Code*).

5 Инкапсуляция зашифрованных данных (ESP)

5.1 Общие требования

Вложение ESP-пакета ДОЛЖНО соответствовать требованиям для вложений комбинированного преобразования определенным в разделе 2 **RFC4303**. Инкапсуляция зашифрованных данных с использованием алгоритма шифрования ГОСТ 28147-89 ДОЛЖНА выполняться с учетом следующих требований:

- синхропосылка (IV) передается в пакете и имеет размер 8 байт;
- ESP-вложение выравнивается по границе 8 байт;
- если согласовано использование ESN, то Seq#h в пакете не передаётся;
- явного выравнивания *ICV* не производится;
- *ICV* передаётся в пакете, имеет размер 4 байта (для преобразования ESP_GOST-4M-IMIT) или 8 байт (для преобразования ESP_GOST-1K-IMIT).

Для согласуемых IPsec SA РЕКОМЕНДУЕТСЯ:

- включать услуги обеспечения защиты от навязывания повторных пакетов (anti-replay);
- если услуга защиты от навязывания повторных пакетов не используется или используется не в полном объёме, РЕКОМЕНДУЕТСЯ ограничить общее количество и суммарный объём ESP-вложений с одинаковым значением *Seq#* дополнительными организационно-техническими мерами.

5.2 Порядок применения ГОСТ 28147-89 для вложений ESP

Ассоциированные данные, участвующие в выработке имитовставки для вложений ESP, ДОЛЖНЫ содержать следующую служебную информацию:

$$A = SPI \mid Seq\#l \mid IV(Seq\#)$$

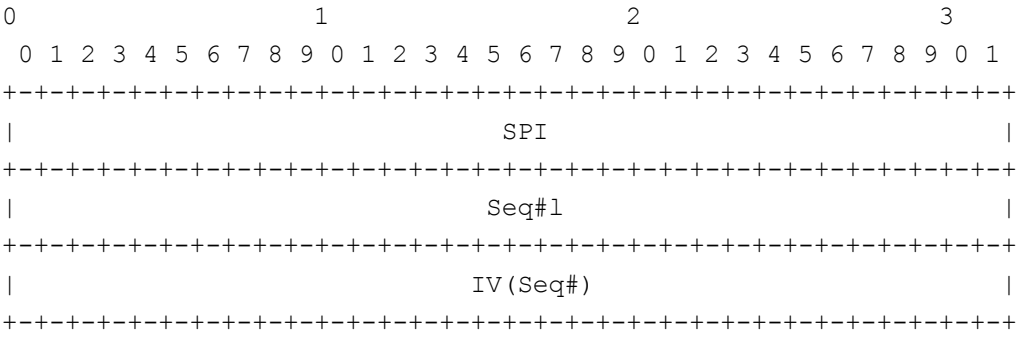

Рисунок 1. Ассоциированные данные (A) для вложений ESP

В преобразованиях используется вектор *IV(Seq#)*, который имеет следующий формат:

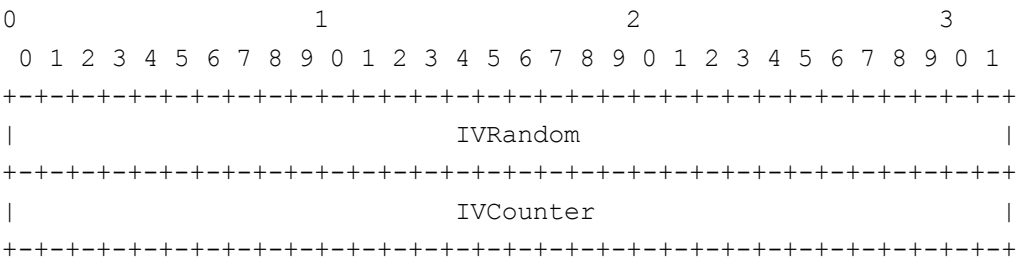

Рисунок 2. Формат IV для ESP_GOST-4M-IMIT и ESP_GOST-1K-IMIT

В этом случае:

IVRandom — случайные 4 байта

$$IVCounter = SPI\text{-}Auth\text{-}Code + SPI + Seq\#l + IVRandom \ (mod\ 2\hat{}32)$$

Получатель ДОЛЖЕН контролировать *IVCounter* на фазе предварительного контроля *Seq#* и НЕ ДОЛЖЕН выполнять криптографических преобразований, если на этапе предварительного контроля выявлена ошибка.

Если реализация ESP поддерживает ведение журналов аудита, то это событие МОЖЕТ классифицироваться как ошибка контроля *Seq#*. В частности, пакеты с ошибочным *IVCounter* НЕ ДОЛЖНЫ вызывать увеличения счётчика искажённых пакетов и уменьшения счетчика объёма данных SA.

5.3 Обработка исходящих пакетов

Порядок обработки исходящих пакетов ДОЛЖЕН соответствовать требованиям, определенным в разделе 3.3 **RFC4303**, со следующими уточнениями:

- дополнительно к проверкам, определенным в разделе 3.3.1 **RFC4303** РЕКОМЕНДУЕТСЯ проверить длину ESP-вложения на соответствие параметрам SA;
- имитовставка в преобразованиях вырабатывается по формуле:

$$substr(0..3, ICV) = gost28147IMIT(0, Kc\_i(Seq\#), A \mid Payload\text{-}Data \mid Padding \mid Pad\text{-}Length \mid Next\text{-}Header\ [\ \mid Seq\#h])$$

- шифрование в преобразовании ESP_GOST-4M-IMIT осуществляется без усложнения ключа;
- шифрование в преобразовании ESP_GOST-1K-IMIT осуществляется в режиме усложнения ключа id-Gost28147-89-CryptoPro-KeyMeshing;
- шифрование в преобразованиях осуществляется по формуле:

$$encryptCNT(IV(Seq\#), Kc\_e(Seq\#), Payload\text{-}Data \mid Padding \mid Pad\text{-}Length \mid Next\text{-}Header)$$

- дополнительная имитовставка в преобразовании ESP_GOST-1K-IMIT вырабатывается по формуле:

$$substr(4..7, ICV) = gost28147IMIT(0, Kc\_i2(Seq\#), A \mid Encrypted\text{-}Payload\ [\ \mid Seq\#h\ ] \mid substr(0..3, ICV))$$

- отправителю РЕКОМЕНДУЕТСЯ увеличить счётчик объёма данных исходящих пакетов для соответствующей SA и сравнить его значение с максимальным объёмом данных этой SA (Lifetime SA, Kbytes). При его превышении РЕКОМЕНДУЕТСЯ заблокировать дальнейшую работу данной SA.

5.4 Обработка входящих пакетов

Порядок обработки входящих пакетов ДОЛЖЕН соответствовать требования, определенным в разделе 3.4 **RFC4303**, со следующими уточнениями:

- дополнительно к проверкам, определенным в разделе 3.4.2 **RFC4303** РЕКОМЕНДУЕТСЯ проверить длину ESP-вложения на соответствие параметрам SA;
- на этапе предварительного контроля пакета для преобразований ESP_GOST-4M-IMIT и ESP_GOST-1K-IMIT РЕКОМЕНДУЕТСЯ выполнять проверку *IV(Seq#)* (раздел 5.2 данного документа);
- на этапе предварительного контроля пакета для преобразования ESP_GOST-1K-IMIT ДОЛЖЕН быть вычислен ICVchk2. Если substr(4..7, ICV) не совпадает с ICVchk2, то получатель ДОЛЖЕН прервать обработку пакета, при этом он НЕ ДОЛЖЕН изменять состояние соответствующей SA и МОЖЕТ не проводить аудит подобных событий, а также НЕ РЕКОМЕНДУЕТСЯ обеспечивать аудит подобных событий без явного на то указания. ICVchk2 вычисляется по формуле:

$$ICVchk2 = gost28147IMIT(0, Kc\_i2(Seq\#), A \mid Encrypted\text{-}Payload\ [\ \mid Seq\#h\ ] \mid substr(0..3, ICV))$$

— получателю РЕКОМЕНДУЕТСЯ увеличить счётчик объёма данных входящих пакетов для соответствующей SA и сравнить его значение с максимальным объёмом данных этой SA (Lifetime SA, Kbytes). При его превышении РЕКОМЕНДУЕТСЯ заблокировать дальнейшую работу данной SA;
— расшифрование в преобразовании ESP_GOST-4M-IMIT осуществляется без усложнения;
— расшифрование в преобразовании ESP_GOST-1K-IMIT осуществляется в режиме усложнения ключа id-Gost28147-89-CryptoPro-KeyMeshing;
— расшифрование в преобразованиях осуществляется по формуле:

decryptCNT(IV(Seq#), Kc_e(Seq#), Encrypted-Payload)

— на этапе проверки имитовставки для преобразований ДОЛЖЕН быть вычислен ICVchk. Если substr(0..3, ICV) не совпадает с ICVchk, то получателю РЕКОМЕНДУЕТСЯ увеличить счётчик искажённых пакетов соответствующей SA и сравнить его с максимальным значением счётчика искажённых пакетов этой SA. При его превышении РЕКОМЕНДУЕТСЯ заблокировать дальнейшую работу данной SA. ICVchk вычисляется по формуле:

ICVchk = gost28147IMIT(0, Kc_i2(Seq#), A | Encrypted-Payload [| Seq#h]
| substr(0..3, ICV))

5.5 Вычисление MTU

При определении MTU с использованием преобразования ESP_GOST-4M-IMIT и ESP_GOST-1K-IMIT следует руководствоваться правилами, описанными в разделе 2 **RFC4303**, производить выравнивание до размера, кратного 8 байтам с учётом фиксированного добавленного размера 12 байт при использовании ESP_GOST-4M-IMIT (8 байт IV плюс 4 байта ICV) или 16 байт при ESP_GOST-1K-IMIT (8 байт IV плюс 8 байт ICV).

5.6 Преобразование ESP_GOST-4M-IMIT

В преобразовании ESP_GOST-4M-IMIT используется:

KeyMeshing = id-Gost28147-89-None-KeyMeshing

Kc_e(Seq#) = Divers(Divers(Divers(Kr_e, Seq#&0xffffffff00000000),
Seq#&0xfffffffffff0000),
Seq#&0xffffffffffffffc0)

Kc_i(Seq#) = Kc_e(Seq#)

5.7 Преобразование ESP_GOST-1K-IMIT

В преобразовании ESP_GOST-1K-IMIT используется:

KeyMeshing = id-Gost28147-89-CryptoPro-KeyMeshing

Kc_e(Seq#) = Divers(Divers(Divers(Kr_e, Seq#&0xffffffff00000000),
Seq#&0xfffffffffff0000),
Seq#)

Kc_i(Seq#) = Kc_e(Seq#)

Kc_i2(Seq#) = Divers(Divers(Divers(Kr_i, Seq#&0xffffffff00000000),
Seq#&0xfffffffffff0000),
Seq#)

6 Дополнительные параметры и атрибуты ESP SA

Для согласования атрибутов преобразований, описанных в данном разделе, при использовании протокола IKE (**RFC2409**) обе стороны ДОЛЖНЫ согласовать идентификатор приложения ESP_GOST_Vendor_ID, который имеет следующий формат:

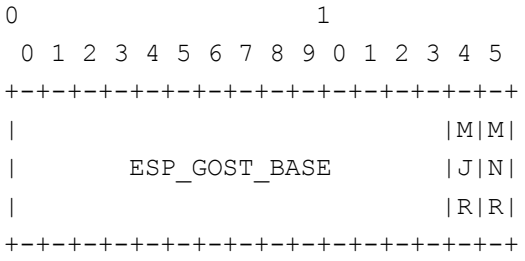

Рисунок 3. Формат ESP_GOST_Vendor_ID

В данном случае, ESP_GOST_BASE = { '\x03', '\x10', '\x17', '\xE0', '\x7F', '\x7A', '\x82', '\xE3', '\xAA', '\x69', '\x50', '\xC9', '\x99', '\x99' } (первые 14 байт значения хэш-функции ГОСТ Р 34.11-94 от char строки "IKE/GOST"), байты MJR и MNR соответствуют текущей major и minor версии преобразований ESP_GOST (т.е. MJR = 1, MNR = 1).

Таблица 1: Параметры ESP SA

Параметр	Атрибут	Формат	Умолчание
Параметры ГОСТ 28147-89	32401	B	—
Максимальный размер пакета	32403	V	65536
Максимальное значение счётчика искажённых пакетов (SA Life Type)	64402	—	10^5

6.1 Параметры ГОСТ 28147-89

При согласовании SA РЕКОМЕНДУЕТСЯ согласовать параметры ГОСТ 28147-89. Класс атрибута: GOST-28147-89-SBOX (32401), формат атрибута: базовый (B).

Таблица 2: Параметры ГОСТ 28147-89

GOST-28147-89 S-box	Значение
id-Gost28147-89-CryptoPro-A-ParamSet	65403
id-Gost28147-89-CryptoPro-B-ParamSet	65404
id-Gost28147-89-CryptoPro-C-ParamSet	65405
id-Gost28147-89-CryptoPro-D-ParamSet	65406

Приложения IPsec, соответствующие требованиям данного документа, ДОЛЖНЫ реализовать набор параметров id-Gost28147-89-CryptoPro-B-ParamSet, который РЕКОМЕНДУЕТСЯ к использованию в сети Интернет. Другие наборы параметров опциональны и МОГУТ применяться в сетях со специальными требованиями (например, при использовании многоуровневого шифрования).

6.2 Максимальное значение счётчиков искажённых пакетов

При достижении максимального значения в счётчике искажённых пакетов ESP SA, определяемого SA-Life-Duration со значением SA-Life-Type = Max-Integrity-Fails, РЕКОМЕНДУЕТСЯ заблокировать обработку пакетов для данной SA и инициировать процедуру её удаления.

6.3 Максимальный размер пакета

Класс атрибута: Max-Packet-Len (32403), формат атрибута: переменная длина (V).

В случае использования протокола ESP с пакетами IPv6 Jumbograms (**RFC2675**) (размерами от 64 Кб до 4 Гб), приложению РЕКОМЕНДУЕТСЯ согласовать параметр максимального размера пакета.

7 Зашифрованные вложения IKEv2

Формирование зашифрованных вложений соответствует требованиям раздела 5.4 ГОСТ 28147-89. Порядок контроля целостности в целом соответствует требованиям раздела 5 **RFC5282** и **RFC5116**, в которых расширяется базовый способ контроля целостности **RFC5996** для случаев использования комбинированных алгоритмов.

Выработка ключевого материала для преобразований ESP осуществляется в соответствии с правилами, определенными в разделе 2.14 **RFC5996**, при этом ключи контроля целостности IKEv2 (*SK_ai* и *SK_ar*) не используются и размер этих ключей ДОЛЖЕН трактоваться как 0 октетов.

Размер ключевого материала для ключей *SK_ei* и *SK_er* соответствует размеру, определенному в разделе 3 **RFC5996**, а именно, 36 или 68 байт для каждого ключа при использовании преобразования ESP_GOST-4M-IMIT или ESP_GOST-1K-IMIT соответственно. При этом, ключевой материал необходимой длины вырабатывается итеративным применением функции PRF без выравнивания на размер значения хэш-функции.

7.1 Порядок применения ГОСТ 28147-89 для вложений IKEv2

Ассоциированные данные, участвующие в выработке имитовставки для вложений IKEv2, ДОЛЖНЫ содержать следующую служебную информацию:

$$A = IKEv2\text{-}Header \mid Unencrypted\text{-}IKE\text{-}Payloads \mid Payload\text{-}Header \mid IV(Seq\#)$$

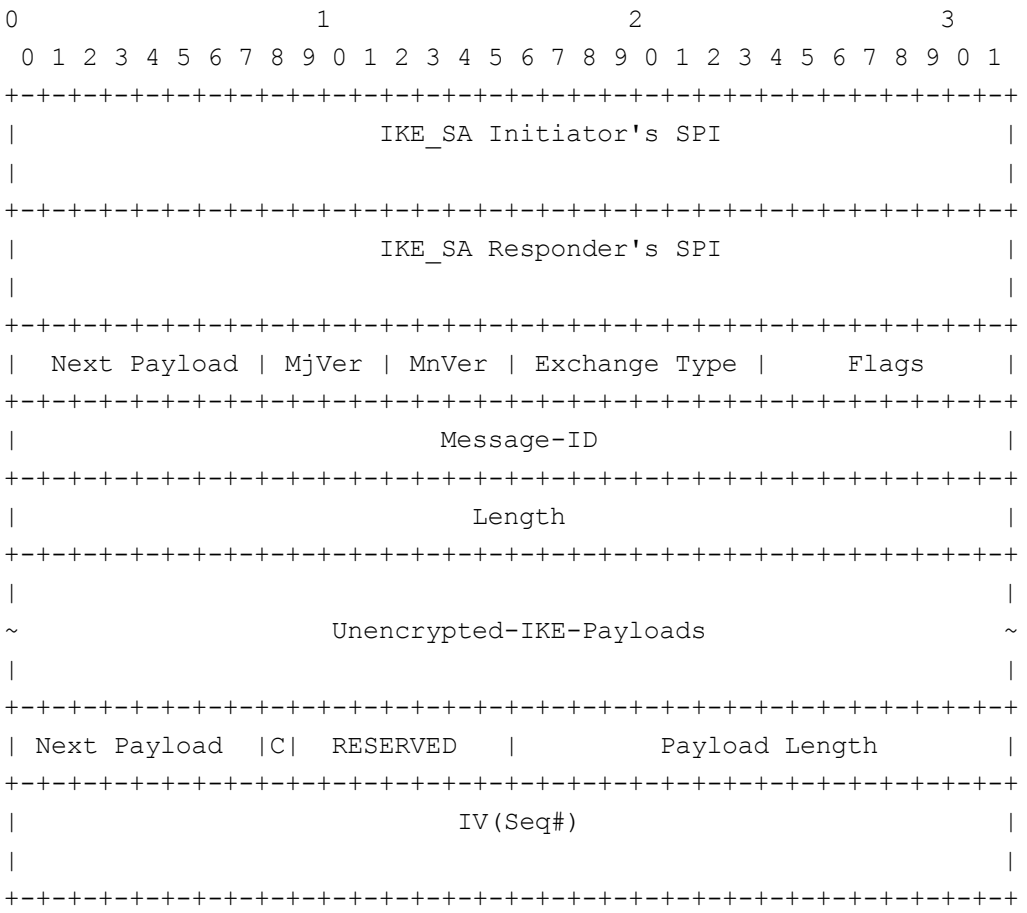

Рисунок 4. Ассоциированные данные (A) для вложений IKEv2

7.2 Выработка IV для вложений IKEv2

В преобразованиях используется вектор IV(Seq#), формат и рекомендации для которого аналогичны IV(Seq#) изложенным в разделе 5.2 данного документа, с учетом следующих уточнений:

$$Seq\# = Message\text{-}ID*2 + R\text{-}flag$$

$$SPI = SPIi\#h + SPIi\#l \text{ (для пакетов от инициатора)}$$

$$SPI = SPIr\#h + SPIr\#l \text{ (для пакетов от респондера)}$$

При применении требований **RFC6311** РЕКОМЕНДУЕТСЯ, либо отказаться от согласования IKEV2_MESSAGE_ID_SYNC_SUPPORTED, либо ограничить количество и суммарный объём второго и последующих пакетов с Message-ID равными 0 (раздел 12 **RFC6311**).

8 Регистрация IANA

IANA выделяет три номера преобразований ESP для использования ГОСТ 28147-89:

<TBD-3> для ESP_GOST-4M-IMIT;

<TBD-4> для ESP_GOST-1K-IMIT

8.1 Удалить после регистрации в IANA

Пока, предварительные реализации используют следующие приватные номера преобразований:

253 для ESP_GOST-4M-IMIT;
252 для ESP_GOST-1K-IMIT.

8.2 Регистрации в IANA не подлежит

Используемые в этом документе приватные номера классов и значений:

Таблица 3. Приватные номера классов ESP SA

Класс	Значение	Тип	Ссылка
GOST-28147-89-SBOX	32401	B	раздел 6.1
Max-Packet-Len	32403	B	раздел 6.3

Используемые в этом документе приватные значения:

Таблица 4: Приватные значения классов ESP SA

Название	Значение	Атрибут
Max-Integrity-Fails	64402	SA-Life-Type, [DOI]
id-Gost28147-89-CryptoPro-A-ParamSet	65403	GOST-28147-89-SBOX, раздел 6.1
id-Gost28147-89-CryptoPro-B-ParamSet	65404	GOST-28147-89-SBOX, раздел 6.1
id-Gost28147-89-CryptoPro-C-ParamSet	65405	GOST-28147-89-SBOX, раздел 6.1
id-Gost28147-89-CryptoPro-D-ParamSet	65406	GOST-28147-89-SBOX, раздел 6.1

9 Рекомендации по безопасному использованию

Приложения РЕКОМЕНДУЕТСЯ исследовать установленным порядком на соответствие заданным требованиям согласно Постановлению Правительства Российской Федерации (ПП РФ №957).

Параметры криптографических алгоритмов влияют на стойкость. Использование параметров, которые не перечислены в **RFC4357**, НЕ РЕКОМЕНДУЕТСЯ без соответствующих исследований, описанных в разделе 9 **RFC4357**.

Поскольку ГОСТ 28147-89 имеет размер блока 64-бит, то для обеспечения конфиденциальности и целостности данных реализациям IPsec РЕКОМЕНДУЕТСЯ соблюдать следующие ограничения:

- для ESP_GOST-4M-IMIT РЕКОМЕНДУЕТСЯ обрабатывать пакеты, не превышающие размера 64 Кбайта. НЕ РЕКОМЕНДУЕТСЯ согласовывать параметр Max-Packet-Len для пакетов IPv6 больший 64 Кбайт, и НЕ РЕКОМЕНДУЕТСЯ использовать IPv6 Jumbograms (**RFC2675**). РЕКОМЕНДУЕТСЯ повторное согласование ключей для нового ESP SA по достижению максимально допустимого объёма данных SA (Lifetime SA) – 2^80 байт;
- для ESP_GOST-1K-IMIT РЕКОМЕНДУЕТСЯ повторное согласование ключей для нового ESP SA по достижению максимально допустимого объёма данных SA (Lifetime SA) - 2^80 байт;
- приложениям РЕКОМЕНДУЕТСЯ согласовывать время жизни SA (Lifetime SA), как по времени, так и по объёму переданной информации (раздел 4.4.2.1 **RFC4301**);

— НЕ РЕКОМЕНДУЕТСЯ согласовывать время жизни SA (Lifetime SA) в секундах более чем на 86400 сек (1 сутки);

— НЕ РЕКОМЕНДУЕТСЯ согласовывать параметр Max-Integrity-Fails больший, чем 10^5, без соответствующего исследования;

— Для приложений с требованиями по уровню защиты КВ1 и выше НЕ РЕКОМЕНДУЕТСЯ согласовывать параметр Max-Integrity-Fails больший, чем 10^1, без соответствующего исследования. Так же, для таких приложений, без соответствующего исследования, НЕ РЕКОМЕНДУЕТСЯ использовать преобразование ESP_GOST-4M-IMIT.

10 Требования по совместимости

Требования по реализации преобразований:

— ESP_GOST-4M-IMIT — обязательно;

— ESP_GOST-1K-IMIT — опционально, требуется при повышенных требованиях к безопасности (КВ1 или выше) или при передаче пакетов IPv6 очень большого размера (более 64 Кбайт);

— id-Gost28147-89-CryptoPro-B-ParamSet — обязательно.

10.1 Совместимость со старыми реализациями IKEv1

Некоторые реализации IKEv1 не полностью совместимы с рекомендациями **RFC6071**, **RFC4301**, **RFC4303** и не поддерживают реализацию поля ICV и его проверки, в случае, если для ESP SA согласован Integrity algorithm "NULL", т.е. если "proposal" не содержит атрибута «Authentication Algorithm» (5).

Такие реализации протокола IKEv1 МОГУТ согласовывать в "proposal" значение атрибута «Authentication Algorithm» (5):

GOST-NULL-INTEGRITY-ALGORITHM - 65411.

Поведение ESP SA в этом случае ДОЛЖНО быть таким же, как при отсутствии атрибута «Authentication Algorithm» (5).

Примеры

Форматы представления данных в примерах:

0xNNNN: Представление целого числа в шестнадцатеричной системе счисления, а также представление объктов в форме big-endian;

0xFFFFFFFF FF...: Представление объектов в форме *big-endian*;

BBBBBBBB BB: Представление объектов в сетевой нотации. Числа в *big-endian*. Сетевое представление сложных объектов согласно стандартам их определяющих, в частности, ключей и хэ-шей согласно **RFC4357**, **RFC4490** и **RFC4490**.

В примерах используются параметры сопоставления безопасности, принятые по умолчанию: шифрование с узлом замены id-Gost28147-89-CryptoPro-B-ParamSet.

A.1. Тестовый пакет ESP_GOST-4M-IMIT

```
 ESP   GOST 4M
 Открытые данные пакета, длина 53:
 4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
 20212223 24252627 28292a2b 2c2d2e2f 30313233 34


SPI
 31323334
Seq#l
 0000007d
 ESN
 не согласован

SPI-Auth-Code
cb4e1a7f
Kr_e
 b63d156f 7aac0dc7 cd915c35 63f61b9d 5c730a74 e331bc8c 3fc24a36 06463893
Kr_e2 = Divers(Kr_e, Seq# & 0xffffffff00000000)
 3a742e54 a9e8a3a1 1f4af5f7 c92fdac1 55142bee 86766e8c 03fad68d 35baf3d7
Kr_e1 = Divers(Kr_e2, Seq# & 0xffffffffffff0000)
 752bdd27 99dcde7b 92c04591 40fac2cb 974f39dc cf589d45 00a67c75 99ff9fcc
Kc_e = Divers(Kr_e1, Seq# & 0xfffffffffffffc0)
 0772fe26 c770590f 22902ad2 1a919eee ccab5396 baf2f1b5 54366c30 27a38614
```

Параметры SA с комбинированным алгоритмом и промежуточные данные ESP_GOST-4M-IMIT:

```
 Промежуточные данные ESP_GOST-4M-IMIT


Seq#
 0000007d
IVRandom
 05060708
IVCounter
 01865538
```

```
 Padding, PadLen, NextProto
 000104
ICV
 0bd8ba08
```

```
 ESP вложение, длина 76
 31323334 0000007d 05060708 01865538 fa104495 3cd50f2b cca22b90 f4f36257
 8f4c2435 f04ada62 d0abc8b3 099e0473 d1ccd142 1586d564 a5e3d1c2 34e529ff
 fe652e24 caad891c 0bd8ba08
```

A.2. Тестовый пакет ESP_GOST-1K-IMIT

```
 ESP   GOST 1K
 Открытые данные пакета, длина 1049:
 4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
 20212223 24252627 28292a2b 2c2d2e2f 30313233 34353637 38393a3b 3c3d3e3f
 40414243 44454647 48494a4b 4c4d4e4f 50515253 54555657 58595a5b 5c5d5e5f
 60616263 64656667 68696a6b 6c6d6e6f 70717273 74757677 78797a7b 7c7d7e7f
 80818283 84858687 88898a8b 8c8d8e8f 90919293 94959697 98999a9b 9c9d9e9f
 a0a1a2a3 a4a5a6a7 a8a9aaab acadaeaf b0b1b2b3 b4b5b6b7 b8b9babb bcbdbebf
 c0c1c2c3 c4c5c6c7 c8c9cacb cccdcecf d0d1d2d3 d4d5d6d7 d8d9dadb dcdddedf
 e0e1e2e3 e4e5e6e7 e8e9eaeb ecedeeef f0f1f2f3 f4f5f6f7 f8f9fafb fcfdfeff
 00010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
 20212223 24252627 28292a2b 2c2d2e2f 30313233 34353637 38393a3b 3c3d3e3f
 40414243 44454647 48494a4b 4c4d4e4f 50515253 54555657 58595a5b 5c5d5e5f
 60616263 64656667 68696a6b 6c6d6e6f 70717273 74757677 78797a7b 7c7d7e7f
 80818283 84858687 88898a8b 8c8d8e8f 90919293 94959697 98999a9b 9c9d9e9f
 a0a1a2a3 a4a5a6a7 a8a9aaab acadaeaf b0b1b2b3 b4b5b6b7 b8b9babb bcbdbebf
 c0c1c2c3 c4c5c6c7 c8c9cacb cccdcecf d0d1d2d3 d4d5d6d7 d8d9dadb dcdddedf
 e0e1e2e3 e4e5e6e7 e8e9eaeb ecedeeef f0f1f2f3 f4f5f6f7 f8f9fafb fcfdfeff
 00010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
 20212223 24252627 28292a2b 2c2d2e2f 30313233 34353637 38393a3b 3c3d3e3f
 40414243 44454647 48494a4b 4c4d4e4f 50515253 54555657 58595a5b 5c5d5e5f
 60616263 64656667 68696a6b 6c6d6e6f 70717273 74757677 78797a7b 7c7d7e7f
 80818283 84858687 88898a8b 8c8d8e8f 90919293 94959697 98999a9b 9c9d9e9f
 a0a1a2a3 a4a5a6a7 a8a9aaab acadaeaf b0b1b2b3 b4b5b6b7 b8b9babb bcbdbebf
 c0c1c2c3 c4c5c6c7 c8c9cacb cccdcecf d0d1d2d3 d4d5d6d7 d8d9dadb dcdddedf
 e0e1e2e3 e4e5e6e7 e8e9eaeb ecedeeef f0f1f2f3 f4f5f6f7 f8f9fafb fcfdfeff
 00010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
 20212223 24252627 28292a2b 2c2d2e2f 30313233 34353637 38393a3b 3c3d3e3f
 40414243 44454647 48494a4b 4c4d4e4f 50515253 54555657 58595a5b 5c5d5e5f
 60616263 64656667 68696a6b 6c6d6e6f 70717273 74757677 78797a7b 7c7d7e7f
 80818283 84858687 88898a8b 8c8d8e8f 90919293 94959697 98999a9b 9c9d9e9f
 a0a1a2a3 a4a5a6a7 a8a9aaab acadaeaf b0b1b2b3 b4b5b6b7 b8b9babb bcbdbebf
 c0c1c2c3 c4c5c6c7 c8c9cacb cccdcecf d0d1d2d3 d4d5d6d7 d8d9dadb dcdddedf
 e0e1e2e3 e4e5e6e7 e8e9eaeb ecedeeef f0f1f2f3 f4f5f6f7 f8f9fafb fcfdfeff
 00010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18
```

Параметры SA с комбинированным преобразованием ESP_GOST-1K-IMIT

```
SPI
```

```
 31323334
Seq#l
 0000007d
 ESN
 согласован

Seq#h
0000000b
SPI-Auth-Code
c4c08a66
Kr_e
 b63d156f 7aac0dc7 cd915c35 63f61b9d 5c730a74 e331bc8c 3fc24a36 06463893
Kr_e2 = Divers(Kr_e, Seq# & 0xffffffff00000000)
 59f1548e a0b38639 c546fb94 2164d780 f075460a cb72e4cf f3068a03 a184d544
Kr_e1 = Divers(Kr_e2, Seq# & 0xffffffffffff0000)
 c210c1fc 6988bb00 6ed69111 9d63a619 6c4cee21 799786db 2af3bda9 c77f9e20
Kc_i = Kc_e = Divers(Kr_e1, Seq#)
 fdcd7812 74018a14 5aee2da7 f21a1581 148378b9 272e3d88 0585ac2e 94b4bbe2
Kr_i
 cb4e1a7f 2d61710d f264423c ad4384de ce01d676 90556865 f1cb7f7f ab4103c0
Kr_i2 = Divers(Kr_i, Seq# & 0xffffffff00000000)
 52aa9784 2ee74f7a 5c3c7436 9fe4f415 5a4bc218 05fc6263 2a1ef408 4d8de3a2
Kr_i1 = Divers(Kr_i2, Seq# & 0xffffffffffff0000)
 7ea6c8f3 209ac480 f181aa61 5c38d07b fd680717 16581ff9 c2963646 6094cc3a
Kc_i2 = Divers(Kr_i1, Seq#)
 138309a0 5813c2bf d3bfb2a9 aff9b511 555c2088 ababcac7 f21f0871 1036aff8


 Промежуточные данные ESP_GOST-1K-IMIT


Seq#
 0000007d
IVRandom
 05060708
IVCounter
 faf8c51f
 Padding, PadLen, NextProto
 00000000 00050400 00000b
ICV
 bb3465d8 eb50af47


 ESP вложение, длина 1080
 31323334 0000007d 05060708 faf8c51f 85bc7a31 676f1453 c167d042 1e87a0d1
 a23cbb97 cefbd7fe e95c3d1a b9f3fa9e 144dc92a 97e6de75 5b1fda97 8436c90b
 289c222f 80de286b bdf190b3 be7f6abb f627c56d 25ecc471 9bc9a5f3 403f1852
 67b43b70 a860b606 625ab17b 839078dd a55c9e76 78388625 27f17ef8 da3c964f
 0e320c68 6e71c9bb e17381d0 321fdfb5 8092f205 2df6d199 90ec758d 31eb6eeb
 3e152d43 89d4d402 9ab77fb4 09fcf757 b4086948 cf9d8843 5a2b21f2 6c41aa5f
 6b881623 be08b64e 4aeaba95 706598f3 5d56ee18 0feafff4 32b35a54 b37a7c77
 6e408d09 65aa2aa4 41f69040 03cec18a e1529416 88afe127 1c0fd90b c9699020
 9a98527f e8d4a285 de2f1d09 3b0f6779 a2391f71 d12d1219 c98b74ce 30b35b04
 381896c5 205ca00b ed4df571 d24ecfd3 7134b910 7c8eeb2d 6e3dedf3 ffab4af1
 1e69b296 fb4a9d0d 3dc364e0 4f0c6ab9 925322e4 0a8ff71e 4281d099 87260500
 bdfbdaf2 7669db9e 5b6021c7 91e77aa9 e7e4fe4a c6cafefc 80ff180b e3ec8d33
```

```
6fb8172f 460daaf0 1f407230 bc282c25 9f14bc46 2d8d972e d27bf894 29696abb
03d37ff0 f4ff8c0b c1f62112 eba15368 218a94ca 16847d57 55522e27 60913848
50e84cbb 75438c26 9d216dee 67f82392 4f90a745 1b62b561 badadf9e d9bd481f
6c8d1152 307e5b3b ead13bea 6b3d0b8b 20c0e17e 84109d55 3c431bb3 20ce8ea1
c69e7cfb d720e186 dd4bbdb0 00008b23 f7271bcd ab1f10f2 009d98d1 66af8d49
bf41d101 7aec62b3 1c4ad813 f3508887 d626f23d 387e5398 0ac70ddb 2a5688b4
97f16918 b75f52ca d70751ce 3df694ff 7a07f6ba c1de8abd 6ff88df4 c48299b5
c3e056ec 28ab6d6b 7cd16a59 4f41617b 8cb3bdff a5819619 348cb287 6bf4dcdd
4985141b 2dd6f25a 49fce6cb b43a3dc3 8ca7dfcc fb3b4eca 4b1750eb 0d9da228
80bedd9a 56d1768e 5e883cb1 282c6746 792a9fe9 2a2eabfd 9e48f25c 25ee1f6e
f75c0d05 8ea213a4 f355cac0 608625f1 d78bc810 7d382ef3 0e87240a 4a4c1b87
0c0714a5 7ddd9d09 e12eaf2d 032a1264 cdaf6feb 52b4f3ea 3abb0304 518a11ec
3086d016 cc81461a 34fe9c5a 112a213d ffee305a 7133184c e05df5aa eabd1d9f
341c2951 a126eabf aad3fd0c 6f81faa4 1ccea61e 9a654dec 266147e4 cf14fed7
17656776 781ac09c 6b1e5650 e0a37e3d 98c7a384 3f3c001f e8e5db0f d9c03490
9775bf74 25cf5f63 5befb502 af14595a 56517525 5c3752d9 2f6c7de7 7e80fb37
b6c7d772 d117e4aa e6b1f3a3 1215889f 02111e63 93bd59cb b263a914 275efa37
8069f230 994564af 9f340363 293286ac 6a97d66b 8045fba9 41f41575 6f52d018
162d445c 2f8e6d47 99d00bf7 f419207f bfc51477 7c217b7d bfe9f660 acdd2c43
b6fcb8fc 37db0f6d 78e29e58 88f35340 18217600 cbae06d1 1f24f66c e3c876b6
5157a1e1 356aeed2 e5f4f5c9 3e4784c2 22678beb a7113bc2 e2de9439 382395c6
9c4d0e84 b900f9e1 88f6ec28 651d9462 bb3465d8 eb50af47
```