Криптографические протоколы

AE-, AEAD-режимы шифрования

Деркач Максим Юрьевич

November 30, 2020

Ссылки

https://www.cs.jhu.edu/~Eastubble/dss/ae.pdf
http://cseweb.ucsd.edu/~mihir/papers/oem.pdf
https://habr.com/en/post/425637/

Введение

AEAD-режим блочного шифрования (Authenticated Encryption with Associated Data) — класс блочных режимов шифрования, при котором часть сообщения шифруется, часть остается открытой, и всё сообщение целиком аутентифицировано.

AEAD пришел на замену режиму AE(Authenticated Encryption), который используется/использовался в таких протоколах как (IPSEC, TLS, SSH...).

AE-режим

Шифрование с проверкой подлинности обеспечивает конфиденциальность и целостность данных для защищаемой информации.

Сущетвует три метода реализации AE-режима:

1. Authentication and Encryption (MacAndEnc)
2. Authentication Then Encryption (MacThenEnc)
3. Encryption Then Authentication (EncThenMac)

Метод	Пример	Реализация	Результат
MacAndEnc	SSH	$h = MAC(m), C = Enc(m)$	$C\|\|h$
MacThenEnc	SSL	$h = MAC(C), C = Enc(m\|\|h)$	C
EncThenMac	IPSEC	$C = Enc(m), h = MAC(C)$	$C\|\|h$

Определения

Неразличимость шифротекста(Ciphertext indistinguishability) - это свойство многих систем шифрования. Если система обладает свойством неразличимости, то злоумышленник не сможет отличить пары шифротекстов, основываясь на открытых текстах, которые они шифруют.

IND-CPA - Неразличимость для атак на основе подобранного открытого текста
IND-CCA - Неразличимость для атак на основе подобранного шифротекста

Определения

IND-CPA

1. Испытатель генерирует ключ K и передает его злоумышленнику.
2. Злоумышленник может выполнить полиномиально ограниченное число шифрований.
3. Злоумышленник представляет два отдельных открытых текста M_0, M_1 испытателю.
4. Испытатель выбирает $b \in \{0, 1\}$ случайным образом и посылает шифротекст $C = E_K(M_b)$ обратно злоумышленнику.
5. Злоумышленник может выполнять любое количество дополнительных вычислений или шифрований, и в конце выводит b.

Криптосистема надёжна в смысле IND-CPA, если любой вероятный злоумышленник за полиномиальное время имеет лишь незначительное "преимущество" в различении шифротекстов над случайным угадыванием.

Определения

IND-CCA

1. -||-
2. Злоумышленник может выполнить полиномиально ограниченное число шифрований и вызовов дешифрования с оракулом на основе произвольных шифротекстов.
3. -||-
4. -||-
5. Злоумышленник может выполнять любое количество дополнительных вычислений или шифрований и:
   - 5.1 (IND-CCA1) злоумышленник не может выполнять дальнейшие расшифрования с оракулом.
   - 5.2 (IND-CCA2) злоумышленник может выполнять дальнейшие вызовы оракула, но не может использовать для этого шифротекст C.
6. -||-

$IND - CCA2 \Rightarrow IND - CCA1 \Rightarrow IND - CPA$

Определения

Неизменяемость шифротекста(Non-Malleability) - это свойство шифрования. Алгоритм шифрования является изменяемым («податливым»), если возможно преобразовать зашифрованный текст в другой зашифрованный текст, который расшифровывается в заданный открытый текст.

Определения

Целостность открытого текста(INT-PTXT) - это свойство означает, что невозможно создать такой шифротекст, что полученый при его расшифровке открытй текст отправитель никогда не отправлял (шифровал).

Целостность открытого текста(INT-CTXT) - это свойство означает, что невозможно создать шифротекст, ранее не созданый отпарвителем, независимо от того, являеться ли базовый секрет(откртый текст) новым.
$INT - CTXT \Rightarrow INT - PTXT$

AE-режим

Сравнение AE-режимов:

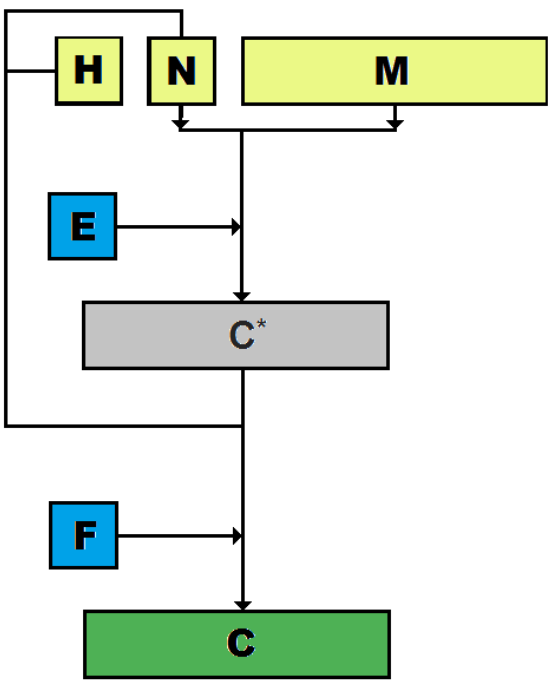
Composition Method	**Privacy**			**Integrity**	
	IND-CPA	IND-CCA	NM-CPA	INT-PTXT	INT-CTXT
Encrypt-and-MAC	insecure	insecure	insecure	secure	insecure
MAC-then-encrypt	secure	insecure	insecure	secure	insecure
Encrypt-then-MAC	secure	secure	secure	secure	secure

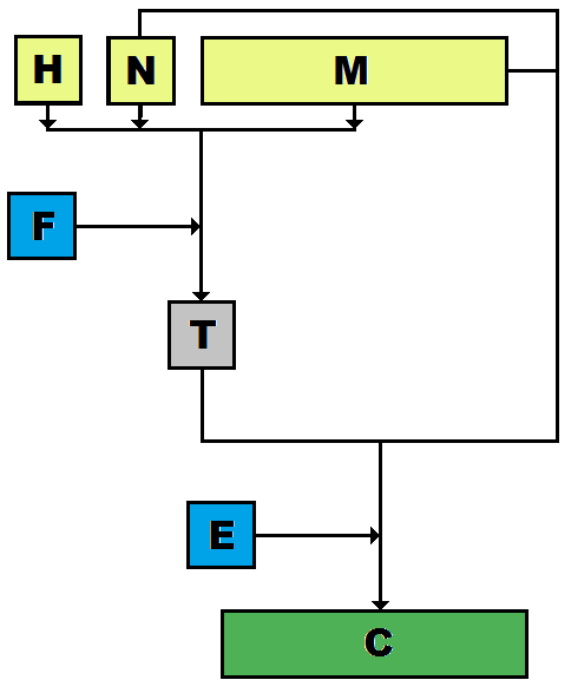
AEAD-режим

Сущетвует 2 метода реализации AE-режима:

1. С помощью алгоритмов EncThenMac и MacThenEnc.
2. С помощью модификации AE-режима.

H - открытый загаловок; M - сообщение; N - nonce; E - симметричная к/с; F - MAC-алгоритм;





AEAD-режим

Примеры модификации AE-режима:

1. Nonce stealing.
   Открытый загаловок передается внутри поля nonce.
2. Ciphertext translation.
   $\hat{E}(K, K_{MAC}, N, M, H) = E_K(N, M) \oplus MAC_{K_{MAC}}(H)$
   $\hat{D}(K, K_{MAC}, N, C, H) = D_K(N, C \oplus MAC_{K_{MAC}}(H))$,
   где E, D - шифрование и дешифрование в режиме AE.