

Технически университет – София



**Изпитен проект по дисциплината
„Семантичен уеб“:**

Криптографски методи за защита на информацията

Изготвил:

Исмаил Осама Салех

ФКСТ, Компютърно и софтуерно инженерство, гр. 223, фак. № 121323039;

Ръководител:

доц. д-р инж. Аделина Алексиева

13.01.2024 г.

1. Област и обхват на онтологията

Каква е областта, която ще се обхваща от онтологията?

Областта на онтологията обхваща съставните части на криптографските методи за защита на информация. Онтологията съответно ще включва описание на тези части, както и техни конкретни изграждащи компоненти и взаимовръзки.

За какво ще се използва онтологията?

Онтологията ще се използва като наричник за основните характеристики и компоненти на криптографията за защита на информация. По този начин се улеснява усвояването на знания, необходими за правилното познаване и прилагане на различните техники.

На какви въпроси отговаря онтологията?

Онтологията дава отговор на следните въпроси:

- Какво е криптографски метод и какви са приложенията му?
- Какви принципи трябва да следва една крипто система?
- Каква е разликата между симетричните и асиметричните криптографски методи?
- Какво е хеш функция и как се използва в криптографията?;
- Какво е алгоритъм за криптиране и как работи?;
- Какво е алгоритъм за декриптиране и как работи?;
- Как се генерират ключове в криптографските методи?;
- Какво е алгоритъм за обмяна на ключове и как работи?;
- Какво е код за удостоверяване на съобщение (MAC) и как се използва в криптографията?;
- Какво е цифров подпис?;
- Какво е блоков шифър и как се различава от поточен шифър? Какви са разликите между тях;
- Каква е връзката между силата на криптографския метод и неговата производителност?;
- Размерът на блока в блоков шифър трябва ли да е равен на размера на ключа, който се използва за криптирането му?;
- Какъв е ефектът от дължината на ключа върху сигурността на един криптографски метод?

Кой ще използва и поддържа онтологията?

Онтологията е подходяща за запознаване на ученици и студенти с основите на криптографските методи за защита на информация. Съответно онтологията служи и като идеална основа за надграждане на базови знания по киберсигурност. Тя притежава публично репо в GitHub, където ентусиасти могат да разглеждат, теглят (клонират или fork-ват) и правят „pull requests (PRs)”. PRs представляват заявки от трети лица към автора/началния разработчик за въвеждане на определени промени в репото. По този начин настоящата разработка се актуализира и от общността освен само от автора.

2. Преизползване на съществуващи онтологии

За направата на текущата онтология не са използвани други цялостни съществуващи онтологии.

3. Ключови термини в онтологията

Класовете, които ще се използват в онтологията и ще изразяват съставните части на криптографските методи за защита на информация, са:

- **CryptographicMethod**- основен клас на онтологията. Показва криптографския метод като обект, свързан чрез обектни свойства с останалите главни класове в йерархията- **AsymmetricCryptographicMethod**, **SymmetricCryptographicMethod**, **HashingFunction**, **MessageAuthenticationCode**, **EncryptionAlgorithm**, **DecryptionAlgorithm**, **KeyGenerationAlgorithm**, **KeyExchangeAlgorithm**.
- **AsymmetricCryptographicMethod**- Асиметричното криптиране използва математически свързана двойка ключове за шифроване и дешифроване: публичен ключ и частен ключ. Ако публичният ключ се използва за шифроване, тогава свързаният с него частен ключ се използва за дешифроване. Ако частният ключ се използва за шифроване, тогава свързаният с него публичен ключ се използва за дешифроване.
- **DigitalSignatureAlgorithm**- Подклас на **AsymmetricCryptographicMethod**. Техниките при цифровите подписи целят осигуряването на автентичност, цялост и неопровержимост за цифровите съобщения или документи.
- **DecryptionAlgorithm**- Декриптирането приема шифротекст и таен ключ като вход. После криптиранта информация (шифротекстът) се преобразува обратно в нейния оригинален вид.
- **EncryptionAlgorithm**- Криптирането е математическа процедура или набор от правила, използвани за преобразуване на четлив текст (некриптирана информация) в криптограм (криптирана информация).
- **HashingFunction**- Функциите тук се използват за преобразуване на данни с произволен размер в такива с фиксиран.
- **KeyExchangeAlgorithm**- Класът съдържа криптографски методи които осъществяват сигурния обмен на криптографски ключове между две страни. Целта на алгоритъма за обмен на ключове е да позволи на две страни да се споразумеят за споделен секретен ключ.
- **KeyGenerationAlgorithm**- Алгоритми за генериране на ключове. Сигурността на много криптографски системи разчита на генерирането на силни и непредсказуеми криптографски ключове.
- **MessageAuthenticationCode**- Включва криптографски техники, използвани за проверка на целостта и автентичността на определено съобщение.
- **BlockCipher**- Блоков шифър.
- **StreamCipher**- Поточен шифър.

Класовете, използвани в онтологията, са свързани помежду си чрез обектни свойства (**Object properties**); Индивидите (**Individuals**) са описани чрез свойства за данни (**Data properties**); Индивид може да се свърже с друг посредством едно или няколко обектни свойства.

Всички обектни свойства са **Functional**, защото един индивид може да притежава една единствена стойност за тях. Те са следните:

- `exchangesKey` – свойство, свързващо класовете `CryptographicMethod` и `KeyExchangeAlgorithm`.
- `generatesKey` – свойство, свързващо класовете `CryptographicMethod` и `KeyGenerationAlgorithm`.
- `isAsymmetric` – свойство, свързващо класовете `CryptographicMethod` и `AsymmetricCryptographicMethod`. Инверсно на `isSymmetric`.
- `isDecryption` – свойство, свързващо класовете `CryptographicMethod` и `DecryptionAlgorithm`.
- `isEncryption` – свойство, свързващо класовете `CryptographicMethod` и `EncryptionAlgorithm`.
- `isHashing` – свойство, свързващо класовете `CryptographicMethod` и `HashingFunction`.
- `isOfTypeMAC` – свойство, свързващо класовете `CryptographicMethod` и `MessageAuthenticationCode`.
- `isSymmetric` – свойство, свързващо класовете `CryptographicMethod` и `SymmetricCryptographicMethod`. Инверсно на `isAsymmetric`.
- `signsDigitalSignature` – свойство, свързващо класовете `AsymmetricCryptographicMethod` и `DigitalSignatureAlgorithm`. Равно е на обектното свойство `verifiesDigitalSignature`, за да се покаже на учениците, че криптографските методи, които генерират цифрови подписи, също служат да ги верифицират в една крипто система.
- `verifiesDigitalSignature` – свойство, свързващо класовете `AsymmetricCryptographicMethod` и `DigitalSignatureAlgorithm`. Равно е на обектното свойство `signsDigitalSignature` поради гореспоменатата причина.

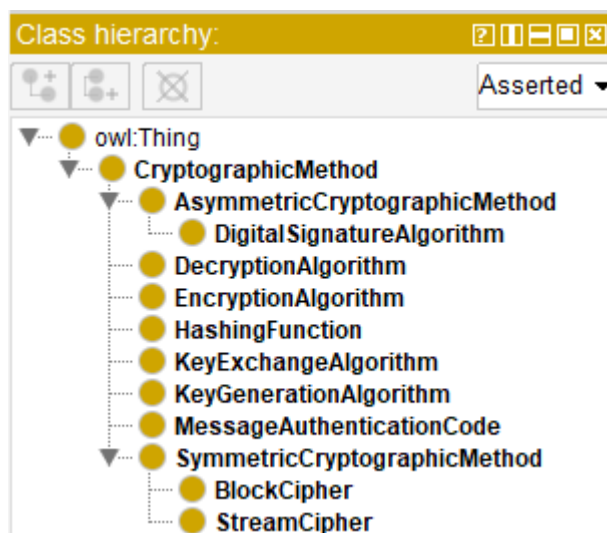
Свойства за данни (data properties) – използват се, за да опишат определен индивид от даден клас чрез определени характеристики. Отново всички са `Functional`.

- `blockSize` (тип: `xsd:integer`) – размер на блок данни в битове.
- `decryptionSpeed` (една от следните стойности: {“high”, “medium”, “slow”}) – скорост на декриптиране.
- `encryptionSpeed` (една от следните стойности: {“high”, “medium”, “slow”}) – скорост на криптиране.
- `hashLength` (тип: `xsd:integer`) – размер на хеш в битове.
- `isPrinciple` (тип: `xsd:boolean`) – дава информация дали индивид е принцип или „актьор“ в криптографските методи.
- `keyLength` (тип: `xsd:integer`) – размер на ключ в битове.
- `securityStrength` (една от следните стойности: {“weak”, “medium”, “strong”, “very strong”}) – сила на сигурност.
- `supportsTweakableBlockEncryption` (тип: `xsd:boolean`) – дали индивид поддържа режим `tweakable-block` криптиране. В този режим различен ключ за всеки блок-данни се използва, което прави криптиращия процес по-устойчив на атаки от вида диференциален криптоанализ и линеен криптоанализ.

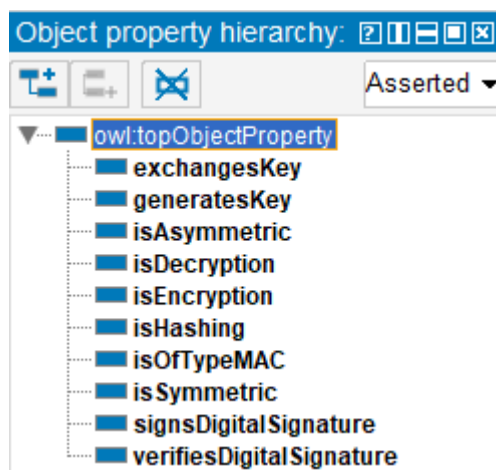
4. Демонстрация чрез графични извадки от онтологията

Ontology metrics:			
Metrics			
Axiom	276		
Logical axiom count	170		
Declaration axioms count	58		
Class count	12		
Object property count	10		
Data property count	8		
Individual count	28		
Annotation Property count	4		
Class axioms			
SubClassOf	11		
EquivalentClasses	0		
DisjointClasses	2		
GCI count	0		
Hidden GCI Count	0		
Object property axioms			
SubObjectPropertyOf	0		
EquivalentObjectProperties	1		
InverseObjectProperties	1		
DisjointObjectProperties	1		
FunctionalObjectProperty	10		
InverseFunctionalObjectProp...	0		
TransitiveObjectProperty	0		
SymmetricObjectProperty	0		
AsymmetricObjectProperty	0		
ReflexiveObjectProperty	0		
IrreflexiveObjectProperty	0		
ObjectPropertyDomain	10		
ObjectPropertyRange	10		
SubPropertyChainOf	0		
Data property axioms			
SubDataPropertyOf	0		
EquivalentDataProperties	0		
DisjointDataProperties	0		
FunctionalDataProperty	8		
DataPropertyDomain	0		
DataPropertyRange	8		
		Individual axioms	
		ClassAssertion	42
		ObjectPropertyAssertion	16
		DataPropertyAssertion	50
		NegativeObjectPropertyAsser...	0
		NegativeDataPropertyAsserti...	0
		SameIndividual	0
		DifferentIndividuals	0
		Annotation axioms	
		AnnotationAssertion	48
		AnnotationPropertyDomain	0
		AnnotationPropertyRangeOf	0

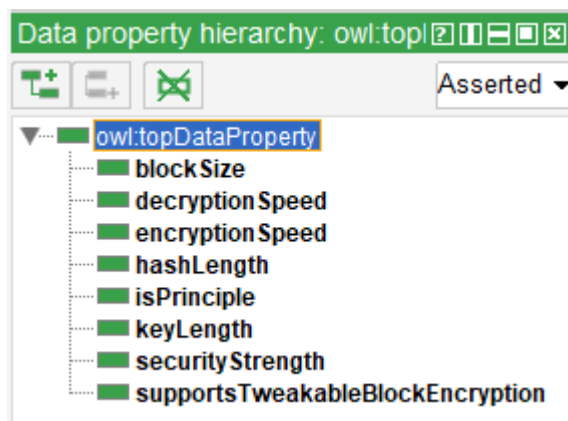
Фиг. 0. Метрики на онтологията.



Фиг. 1. Класова йерархия на онтологията.



Фиг. 2. Обектни свойства на онтологията.



Фиг. 3. Свойства за данни.



Фиг. 4. Индивиди в онтологията.

Nota bene: Предстоят скрийншоти на класове. Ще забележите, че някои класове притежават зачеркнати инстанции. Това е така, защото съответните инстанции притежават „deprecated” анотация.

AsymmetricCryptographicMethod — http://www.semanticweb.org/ism:

Annotations
Usage

Annotations: AsymmetricCryptographicMethod

Annotations
+

rdfs:comment [type: xsd:string]

Asymmetric encryption uses a mathematically related pair of keys for encryption and decryption: a public key and a private key. If the public key is used for encryption, then the related private key is used for decryption. If the private key is used for encryption, then the related public key is used for decryption.

Description: AsymmetricCryptographicMethod

Equivalent To
+

SubClass Of
+

CryptographicMethod

General class axioms
+

SubClass Of (Anonymous Ancestor)

Instances
+

Diffie-Hellman

RSA

Target for Key
+

Disjoint With
+

SymmetricCryptographicMethod

Фиг. 6. Клас *AsymmetricCryptographicMethod*.

⌵ ● DigitalSignatureAlgorithm — http://www.semanticweb.org/ismail/ontc

Annotations Usage

Annotations: DigitalSignatureAlgorithm ? || ▢ ✕

Annotations +

[rdfs:comment](#) @ ✕ ○

A cryptographic technique used to provide authenticity, integrity, and non-repudiation to digital messages or documents. It involves the use of asymmetric-key cryptography, where a pair of cryptographic keys (public key and private key) is employed.

Description: DigitalSignatureAlgorithm ? || ▢ ✕

Equivalent To +

SubClass Of +

● AsymmetricCryptographicMethod ? @ ✕ ○

General class axioms +

SubClass Of (Anonymous Ancestor)

Instances +

◆ RSA_SHA256 ? @ ✕

Фиг. 7. Клас *DigitalSignatureAlgorithm*.

DecryptionAlgorithm — <http://www.semanticweb.org/ismail/ontologies/2024/0/crypto#De>

Annotations Usage

Annotations: DecryptionAlgorithm

Annotations +

rdfs:comment

The complementary process to the encryption algorithm. It takes the ciphertext and the secret key as inputs and transforms the encrypted data back into its original plaintext form. The main goal of a decryption algorithm is to reverse the effects of the encryption process, restoring the original information from the ciphertext.

Asserted in: <http://www.semanticweb.org/ismail/ontologies/2024/0/crypto>

Description: DecryptionAlgorithm

Equivalent To +

SubClass Of +

CryptographicMethod

General class axioms +

SubClass Of (Anonymous Ancestor)

Instances +

AES-256	?	@	×
Blowfish	?	@	×
RSA	?	@	×
Threefish	?	@	×
XOR	?	@	×

Фиг. 8. Клас *DecryptionAlgorithm*.

SymmetricCryptographicMethod — http://www.semanticweb.org/ismail/

Annotations
Usage

Annotations: SymmetricCryptographicMethod

Annotations
+

rdfs:comment [type: xsd:string]

Symmetric cryptography, known also as secret key cryptography, is the use of a single shared secret to share encrypted data between parties. Ciphers in this category are called symmetric because you use the same key to encrypt and to decrypt the data.

Description: SymmetricCryptographicMethod

Equivalent To
+

SubClass Of
+

CryptographicMethod

General class axioms
+

SubClass Of (Anonymous Ancestor)

Instances
+

AES-256

Blowfish

HMAC

Threefish

Target for Key
+

Disjoint With
+

AsymmetricCryptographicMethod

Фиг. 13. Клас *SymmetricCryptographicMethod*.

StreamCipher

http://www.semanticweb.org/ismail/ontologies/2024/0/c

Annotations

Usage

Annotations: StreamCipher

?

||

≡

□

×

Annotations

+

rdfs:comment

@

×

○

Stream ciphers are used for encrypting data in real-time. They use a pseudorandom keystream to encrypt the plaintext. The keystream is generated using a secret key and a feedback mechanism. The feedback mechanism can be a linear feedback shift register (LFSR), a Feistel network, or a Lai-Massey construction.

Stream ciphers do not use hashing algorithms, which are used to create a fixed-size hash value from a variable-size message. Hashing algorithms are used for message authentication and integrity, while stream ciphers are used for encryption.

Description: StreamCipher

?

||

≡

□

×

Equivalent To

+

SubClass Of

+

SymmetricCryptographicMethod

?

@

×

○

General class axioms

+

SubClass Of (Anonymous Ancestor)

Instances

+

StreamCipher-1

?

@

×

StreamCipher-2

?

@

×

Target for Key

+

Disjoint With

+

BlockCipher

?

@

×

○

Фиг. 15. Клас StreamCipher.

☒ Functional
 ☐ Inverse function
 ☐ Transitive
 ☐ Symmetric
 ☐ Asymmetric
 ☐ Reflexive
 ☐ Irreflexive

Description: exchangesKey

Equivalent To +

SubProperty Of +

Inverse Of +

Domains (intersection) +

CryptographicMethod

Ranges (intersection) +

KeyExchangeAlgorithm

☒ Functional
 ☐ Inverse function
 ☐ Transitive
 ☐ Symmetric
 ☐ Asymmetric
 ☐ Reflexive
 ☐ Irreflexive

Description: generatesKey

Equivalent To +

SubProperty Of +

Inverse Of +

Domains (intersection) +

CryptographicMethod

Ranges (intersection) +

KeyGenerationAlgorithm

☒ Functional
 ☐ Inverse function
 ☐ Transitive
 ☐ Symmetric
 ☐ Asymmetric
 ☐ Reflexive
 ☐ Irreflexive

Description: isAsymmetric

Equivalent To +

SubProperty Of +

Inverse Of +

isSymmetric

Domains (intersection) +

CryptographicMethod

Ranges (intersection) +

AsymmetricCryptographicMethod

Disjoint With +

isSymmetric

☒ Functional
 ☐ Inverse function
 ☐ Transitive
 ☐ Symmetric
 ☐ Asymmetric
 ☐ Reflexive
 ☐ Irreflexive

Description: isDecryption

Equivalent To +

SubProperty Of +

Inverse Of +

Domains (intersection) +

CryptographicMethod

Ranges (intersection) +

DecryptionAlgorithm

☒ Functional
 ☐ Inverse function
 ☐ Transitive
 ☐ Symmetric
 ☐ Asymmetric
 ☐ Reflexive
 ☐ Irreflexive

Description: isEncryption

Equivalent To +

SubProperty Of +

Inverse Of +

Domains (intersection) +

CryptographicMethod

Ranges (intersection) +

EncryptionAlgorithm

☒ Functional
 ☐ Inverse function
 ☐ Transitive
 ☐ Symmetric
 ☐ Asymmetric
 ☐ Reflexive
 ☐ Irreflexive

Description: isHashing

Equivalent To +

SubProperty Of +

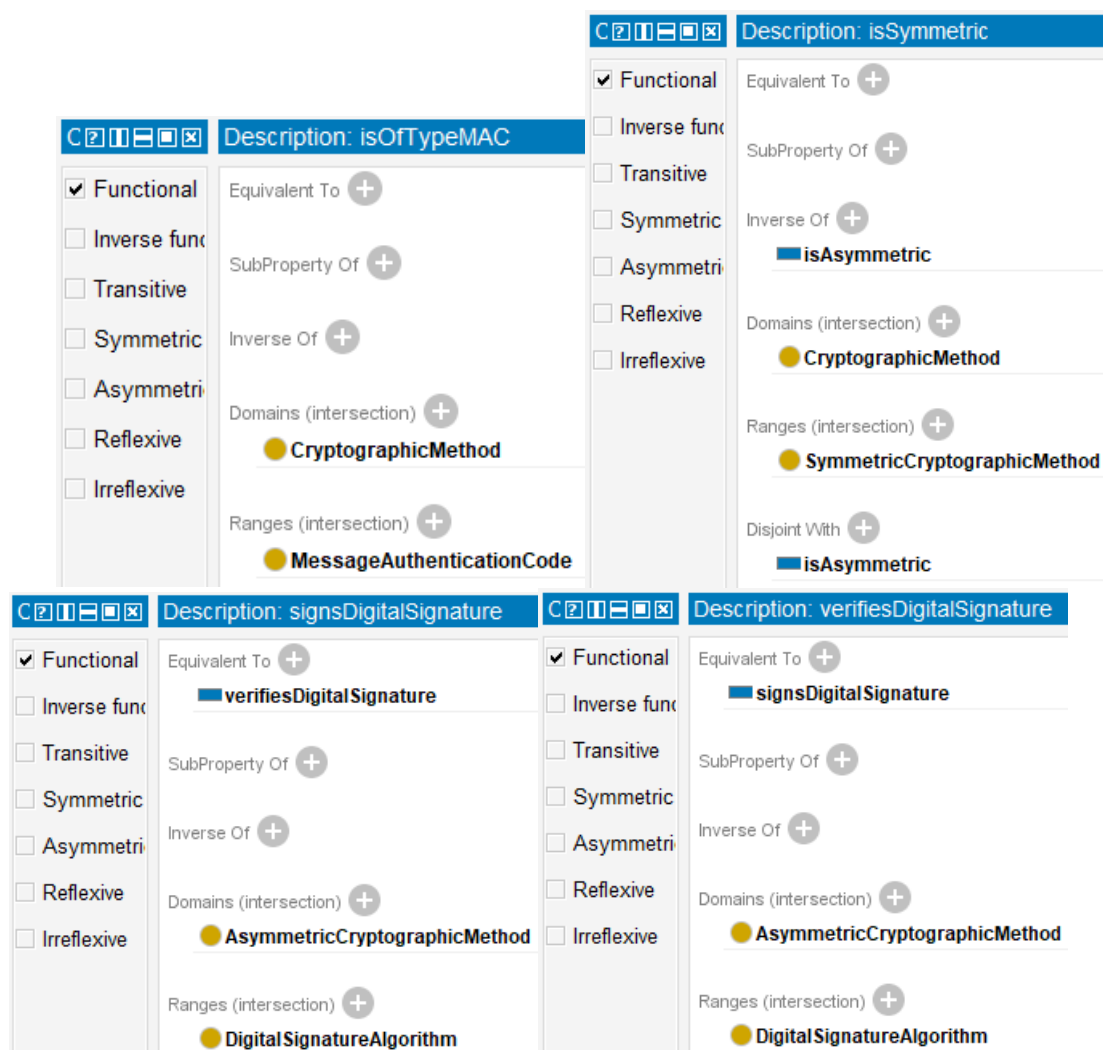
Inverse Of +

Domains (intersection) +

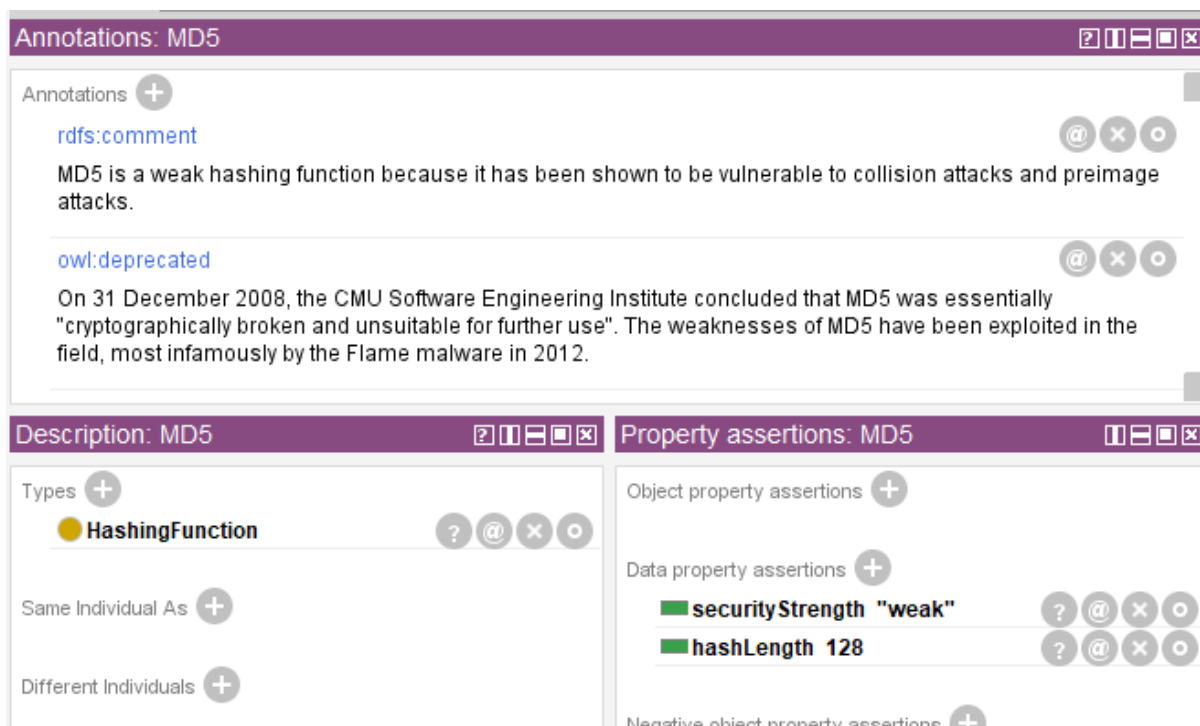
CryptographicMethod

Ranges (intersection) +

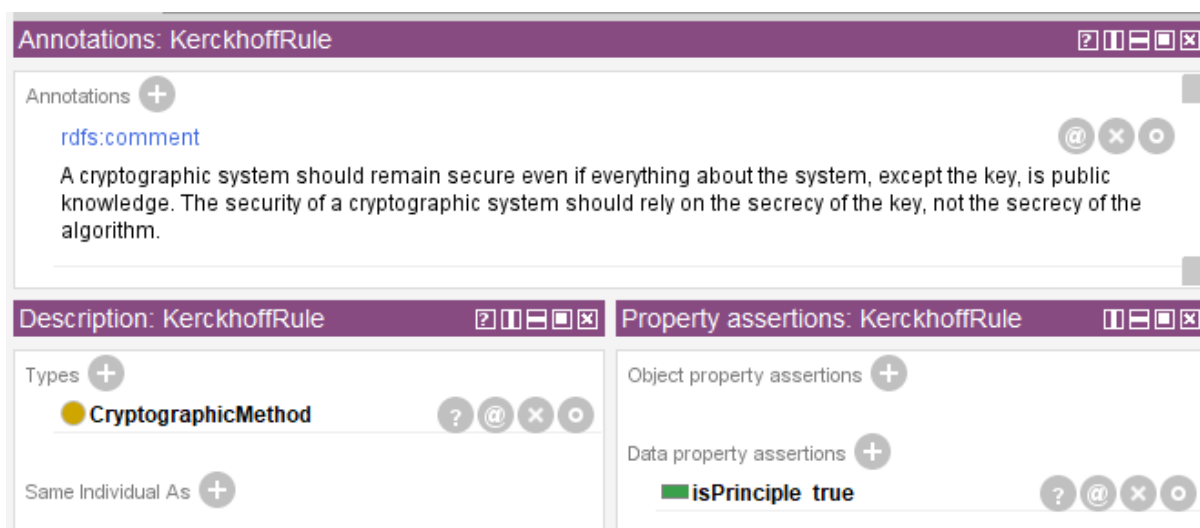
HashingFunction



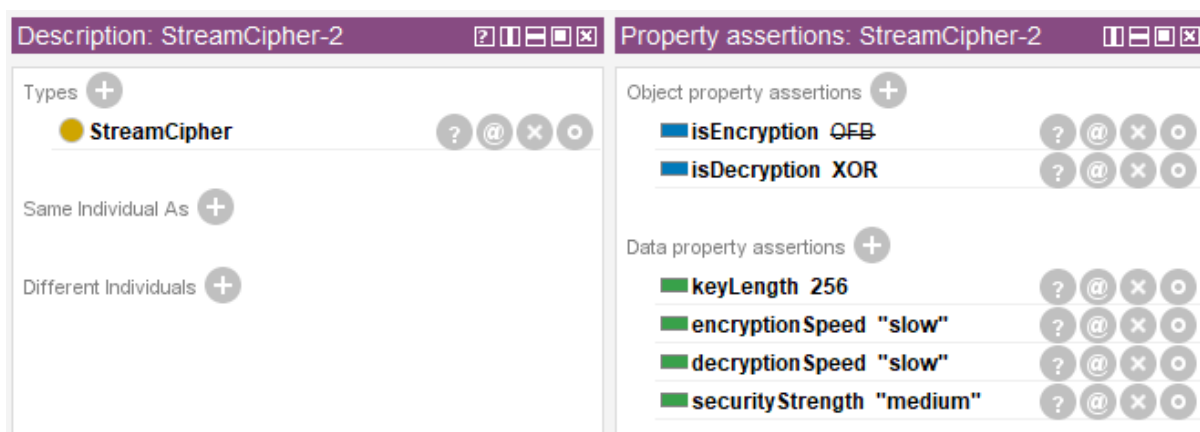
Фиг. 16. Обектните свойства на онтологията – разгърнати.



Фиг. 17. Deprecated индивид – MD5.



Фиг. 18. Индивид, представящ принцип в криптографските методи за защита на информацията.



Фиг. 19. Индивид, представящ примерен поточен шифър.

Annotations: HMAC

Annotations +

rdfs:comment

The hash function used within HMAC typically does not have a specific "blockSize" parameter in the same way as a block cipher. HMAC operates as follows:

1. Key Padding: If the key is shorter than the block size of the hash function, it is padded to match the block size.

2. Inner Hash: The key is XORed with an inner padding value, and the result is hashed along with the message.

3. Outer Hash: The hashed result from the inner step is XORed with an outer padding value, and the final result is hashed again.

The security of HMAC relies on the underlying hash function's properties, such as collision resistance and preimage resistance. HMAC doesn't directly expose or specify the block size of the hash function it uses. Instead, it adapts to the block size of the chosen hash function.

rdfs:comment

Typically, the key length for HMAC would also be 512 bits to match the hash function's output length.

Description: HMAC

Types +

HashingFunction

MessageAuthenticationCode

SymmetricCryptographicMethod

Same Individual As +

Different Individuals +

Property assertions: HMAC

Object property assertions +

isHashing SHA3-512

Data property assertions +

hashLength 512

securityStrength "very strong"

keyLength 512

encryptionSpeed "high"

decryptionSpeed "high"

Фиг. 20. Индивид HMAC.

Annotations: AES-256

Annotations +

rdfs:label

AES-256

rdfs:comment

A widely used symmetric-key algorithm.

rdfs:comment

The original name of this individual is AES. However, I wanted to use this individual in order to represent a specific variant of AES with a key length of 256. So I used the annotation rdfs:label in order to rename the individual to AES-256.

Description: AES-256

Types +

DecryptionAlgorithm

EncryptionAlgorithm

KeyGenerationAlgorithm

SymmetricCryptographicMethod

Property assertions: AES-256

Object property assertions +

Data property assertions +

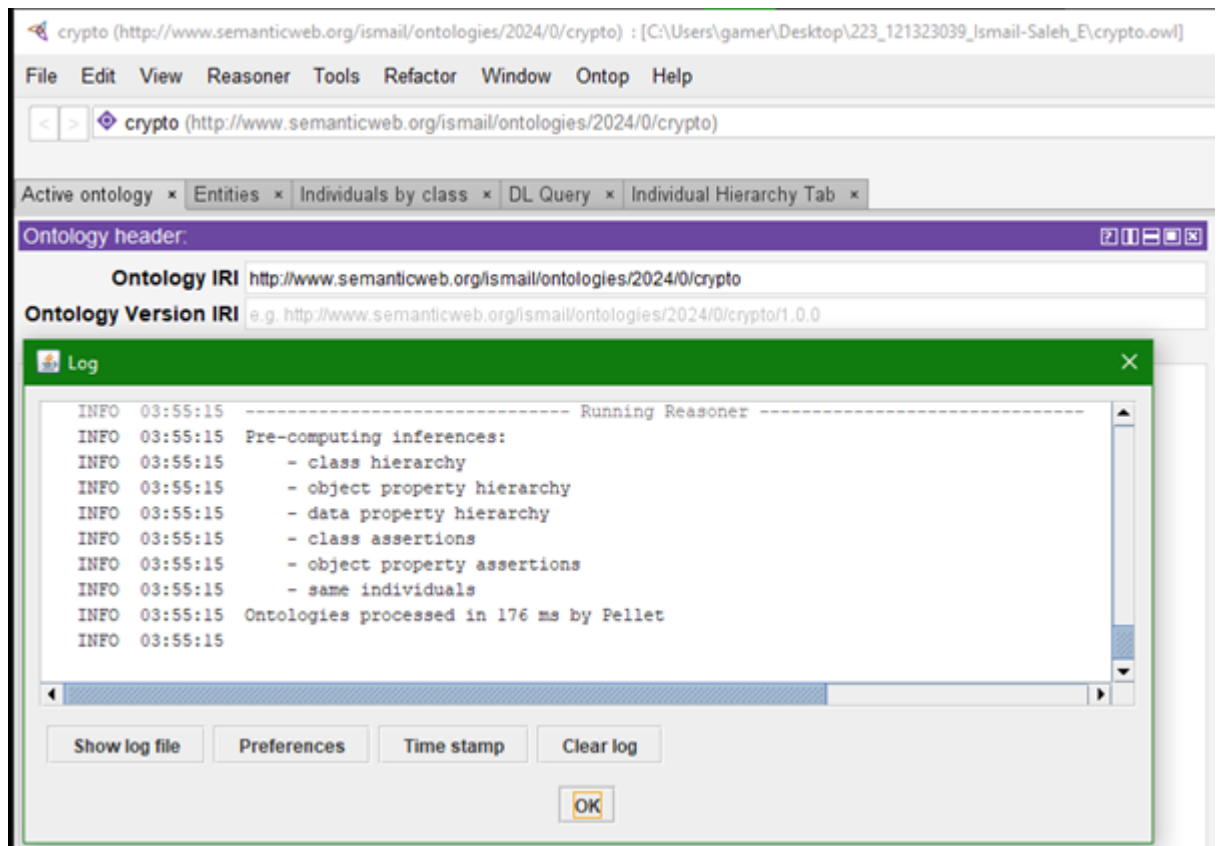
supportsTweakableBlockEncryption false

keyLength 256

Фиг. 21. Индивид, където използвам анотацията rdfs:label с цел да коригирам първоначалното възложено име.

Страница 23 от 27

5. Валидиране на логиката на онтологията чрез reasoner – Pellet



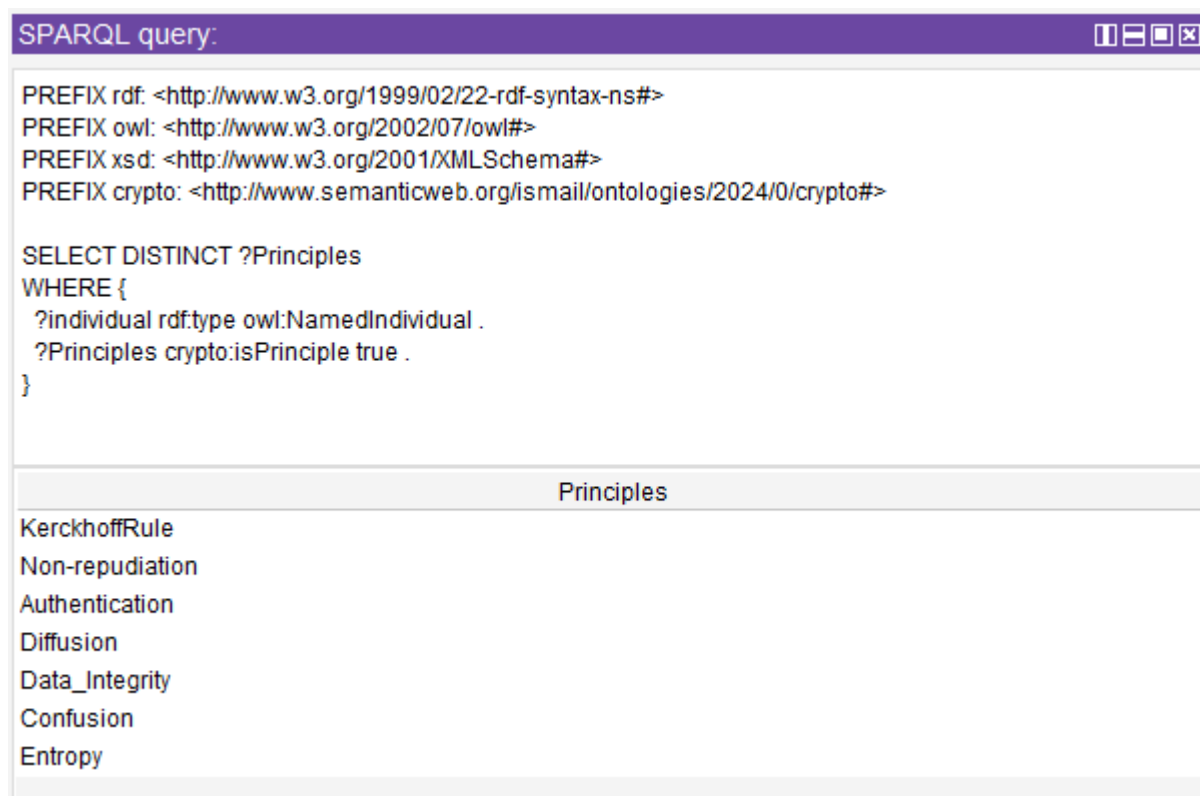
Фиг. 22. Pellet Reasoner изход.

6. SPARQL заявки

1. Извежда се като резултат всички индивиди, които са принципи (чрез свойството за данни isPrinciple):

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX crypto: <http://www.semanticweb.org/ismail/ontologies/2024/0/crypto#>

SELECT DISTINCT ?Principles
WHERE {
  ?individual rdf:type owl:NamedIndividual .
  ?Principles crypto:isPrinciple true .
}
```

Фиг. 23. Изход на първата заявка през Protégé.

2. Извежда се като изход всички блокови шифри, техните алгоритми за криптиране и декриптиране и сила на сигурност:

```

PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX crypto: <http://www.semanticweb.org/ismail/ontologies/2024/0/crypto#>

SELECT ?blockCipher ?encryption ?decryption ?securityStrength
WHERE {
  ?blockCipher rdf:type crypto:BlockCipher .
  ?blockCipher crypto:isEncryption ?encryption .
  ?blockCipher crypto:isDecryption ?decryption .
  ?blockCipher crypto:securityStrength ?securityStrength .
}

```

SPARQL query:			
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> PREFIX owl: <http://www.w3.org/2002/07/owl#> PREFIX xsd: <http://www.w3.org/2001/XMLSchema#> PREFIX crypto: <http://www.semanticweb.org/ismail/ontologies/2024/0/crypto#> SELECT ?blockCipher ?encryption ?decryption ?securityStrength WHERE { ?blockCipher rdf:type crypto:BlockCipher . ?blockCipher crypto:isEncryption ?encryption . ?blockCipher crypto:isDecryption ?decryption . ?blockCipher crypto:securityStrength ?securityStrength . }			
blockCipher	encryption	decryption	securityStrength
BlockCipher-2	Blowfish	Blowfish	"strong"
BlockCipher-3	Threefish	Threefish	"very strong"
BlockCipher-1	AES-256	AES-256	"strong"

Фиг. 24. Изход на втората заявка в Protégé.

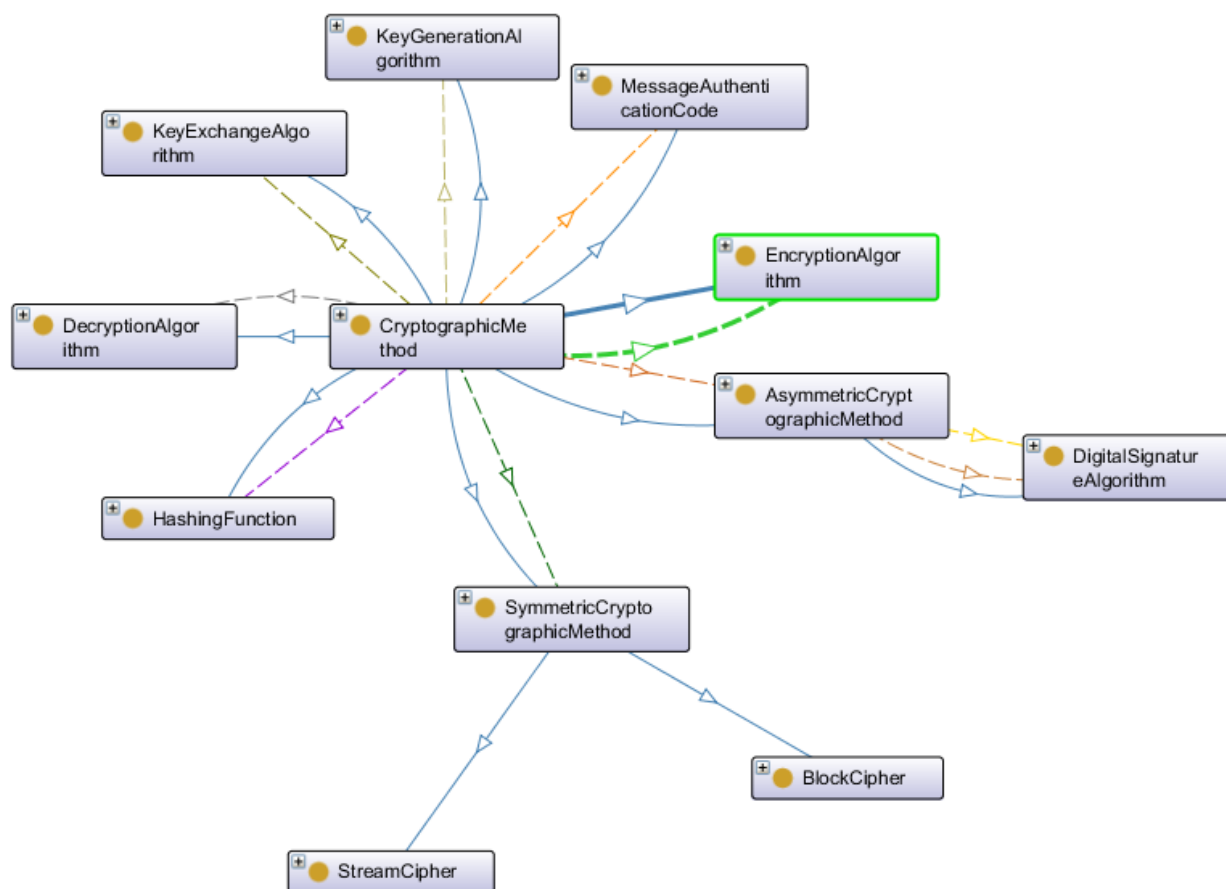
3. Извежда всички хеш функции, дължината на digest-а (изхода), размер на блока и сила на защита:

PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> PREFIX crypto: <http://www.semanticweb.org/ismail/ontologies/2024/0/crypto#> SELECT ?hashingFunction ?hashLength ?blockSize ?securityStrength WHERE { ?hashingFunction rdf:type crypto:HashingFunction . ?hashingFunction crypto:hashLength ?hashLength . ?hashingFunction crypto:blockSize ?blockSize . ?hashingFunction crypto:securityStrength ?securityStrength . }			
---	--	--	--

SPARQL query:			
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> PREFIX crypto: <http://www.semanticweb.org/ismail/ontologies/2024/0/crypto#> SELECT ?hashingFunction ?hashLength ?blockSize ?securityStrength WHERE { ?hashingFunction rdf:type crypto:HashingFunction . ?hashingFunction crypto:hashLength ?hashLength . ?hashingFunction crypto:blockSize ?blockSize . ?hashingFunction crypto:securityStrength ?securityStrength . }			
hashingFunction	hashLength	blockSize	securityStrength
SHA-256	"256" ^{^^} <http://www.w3.org/2001/XMLSchema#integer>	"512" ^{^^} <http://www.w3.org/2001/XMLSchema#integer>	"strong"
MD5	"128" ^{^^} <http://www.w3.org/2001/XMLSchema#integer>	"512" ^{^^} <http://www.w3.org/2001/XMLSchema#integer>	"weak"
SHA3-512	"512" ^{^^} <http://www.w3.org/2001/XMLSchema#integer>	"1088" ^{^^} <http://www.w3.org/2001/XMLSchema#integer>	"very strong"
SHA-512	"512" ^{^^} <http://www.w3.org/2001/XMLSchema#integer>	"1024" ^{^^} <http://www.w3.org/2001/XMLSchema#integer>	"very strong"

Фиг. 25. Изход на третата заявка в Protégé.

7. Графичен модел на онтологията



Фиг. 26. Графичен модел на онтологията.