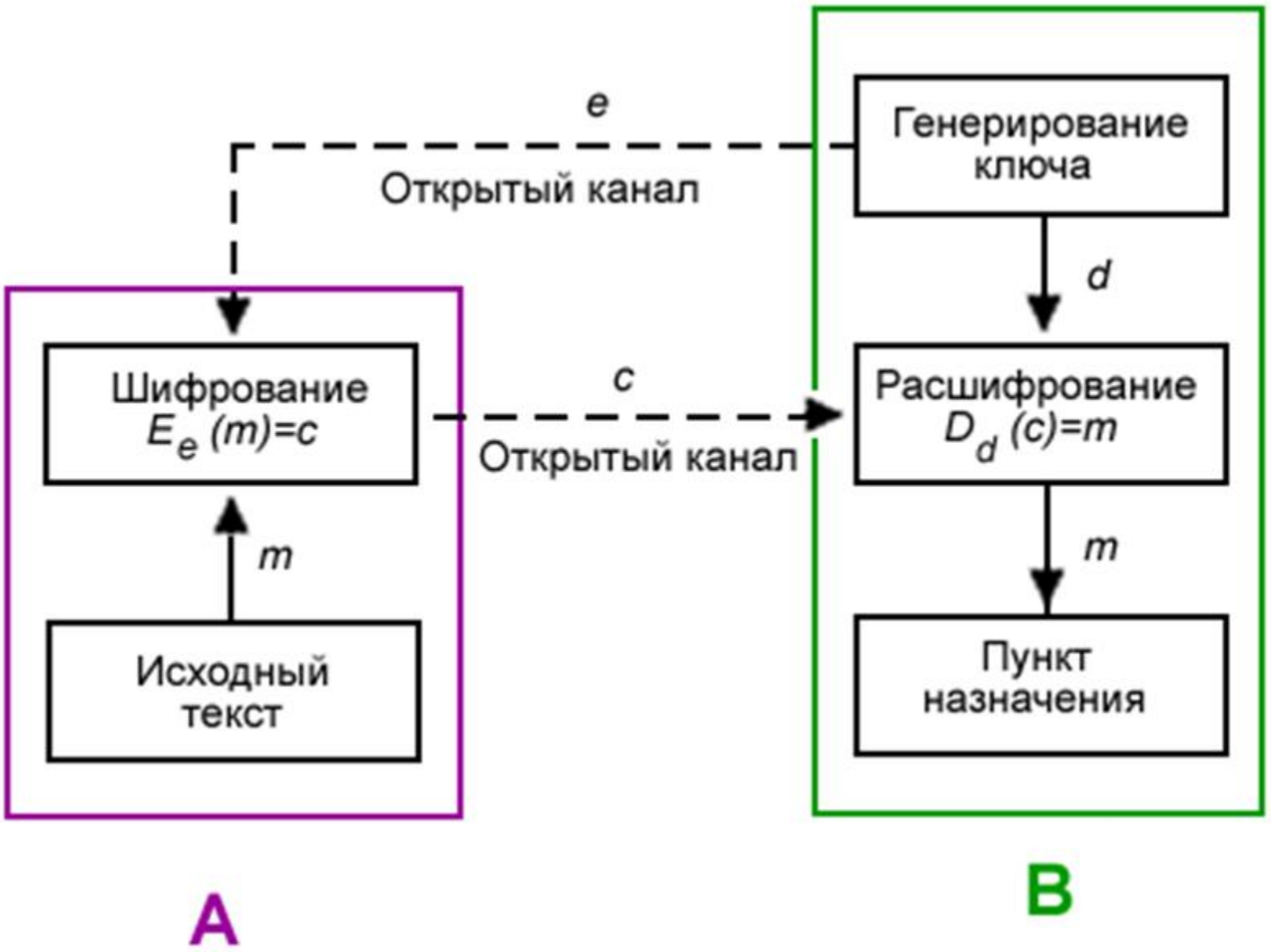
Лекция 6. Служба DNS, дополнительные возможности

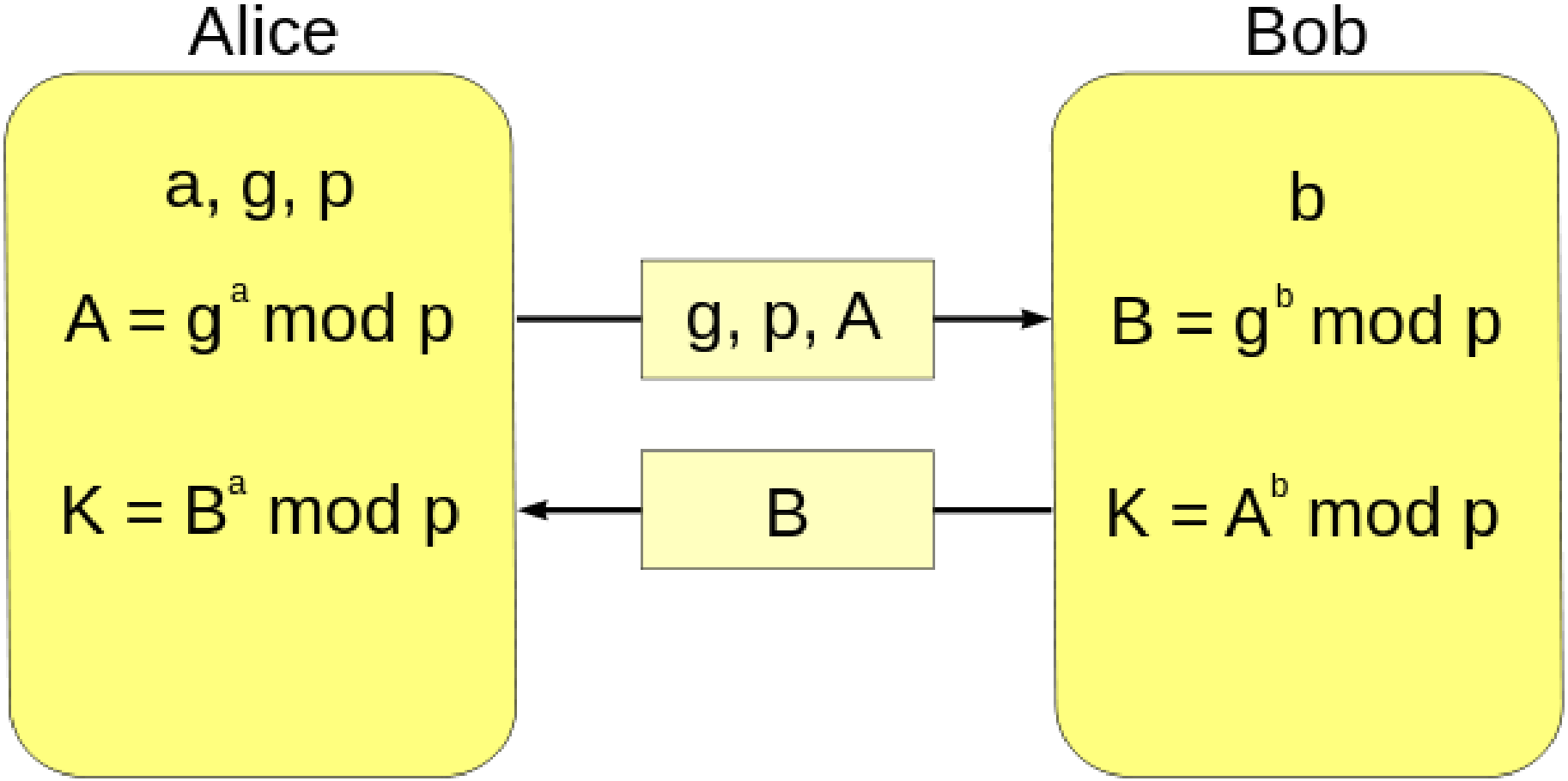
Содержание

1. Основы асимметричной криптографии
2. DNSSEC
3. Интернациональные доменные имена
4. Новые ресурсные записи

Криптосистемы с открытым ключом



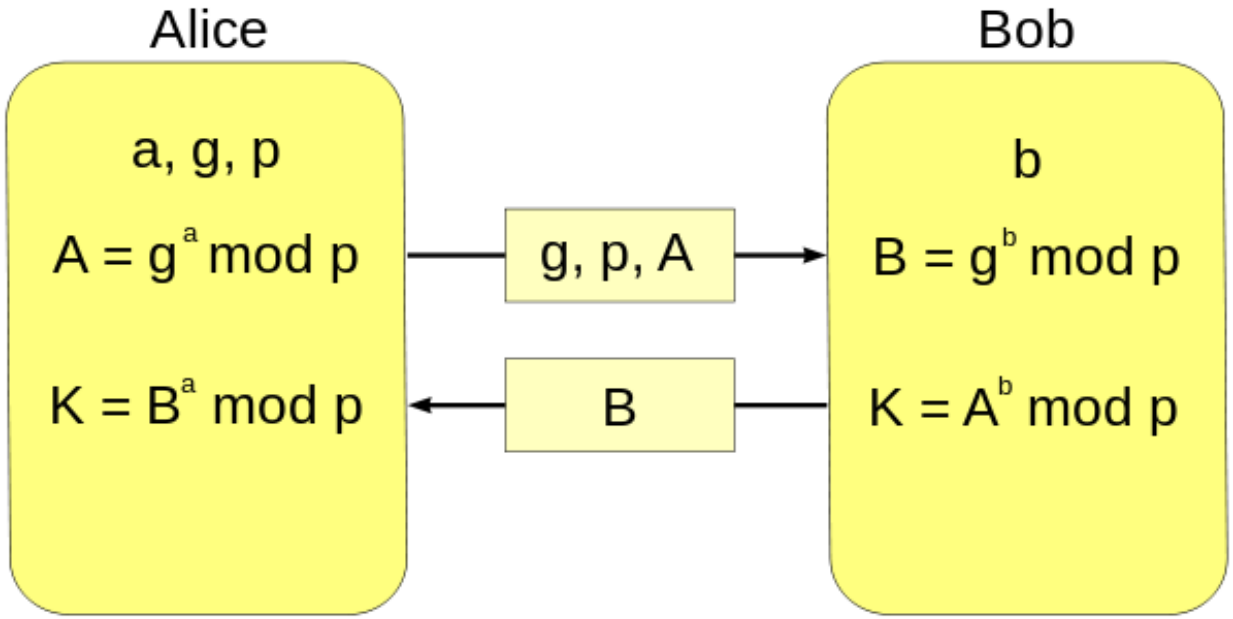
Алгоритм Diffie-Hellman, 1976 г.



$K = A^b \bmod p = (g^{ab}) \bmod p = B^a \bmod p$

Пример работы алгоритма Диффи — Хеллмана

Alice	Bob
$p = 23, g = 5$	$p = 23, g = 5$
$\mathbf{a = 6}$	$\mathbf{b = 15}$
$A = 5^{6} \bmod 23 = 8$	$B = 5^{15} \bmod 23 = 19$
$\mathbf{K} = 19^{6} \bmod 23 = \mathbf{2}$	$\mathbf{K} = 8^{15} \bmod 23 = \mathbf{2}$
$\mathbf{K} = 19^{6} \bmod 23 = 8^{b} \bmod 23$	$\mathbf{K} = 8^{15} \bmod 23 = 19^{a} \bmod 23$



Rivest, Shamir и Adleman

RSA — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

По состоянию на 23 марта 2015 года, наибольшее известное простое число равняется $2^{57885161} - 1$ и содержит 17 425 170 десятичных цифр

1. Выбираются два различных случайных простых числа p, q.

2. $n = p * q$

3. $\Phi(n) = (p-1) * (q-1)$

4. Выбирается целое число e, взаимно простое со значением функции $\Phi(n)$.

Число e называется открытой экспонентой

5. Выбирается целое число d. $d * e \bmod \Phi(n) = 1$

Число называется секретной экспонентой.

6. Пара {e, n} – открытый ключ RSA

7. Пара {d, n} – закрытый ключ RSA

Пример работы RSA

Зашифруем и расшифруем сообщение "CAB" по алгоритму RSA. Для простоты возьмем небольшие числа: p=3 и q=11.

Определим n= 3*11 = 33.

Ф(n) = (p-1)*(q-1)=20.
Пусть e будет равно, например, 3: (e=3).

Находим d: (d*3) mod 20 = 1. Ясно, что d = 7,
т. к. по теореме Эйлера d = e ^(Ф(n)-1) mod n.

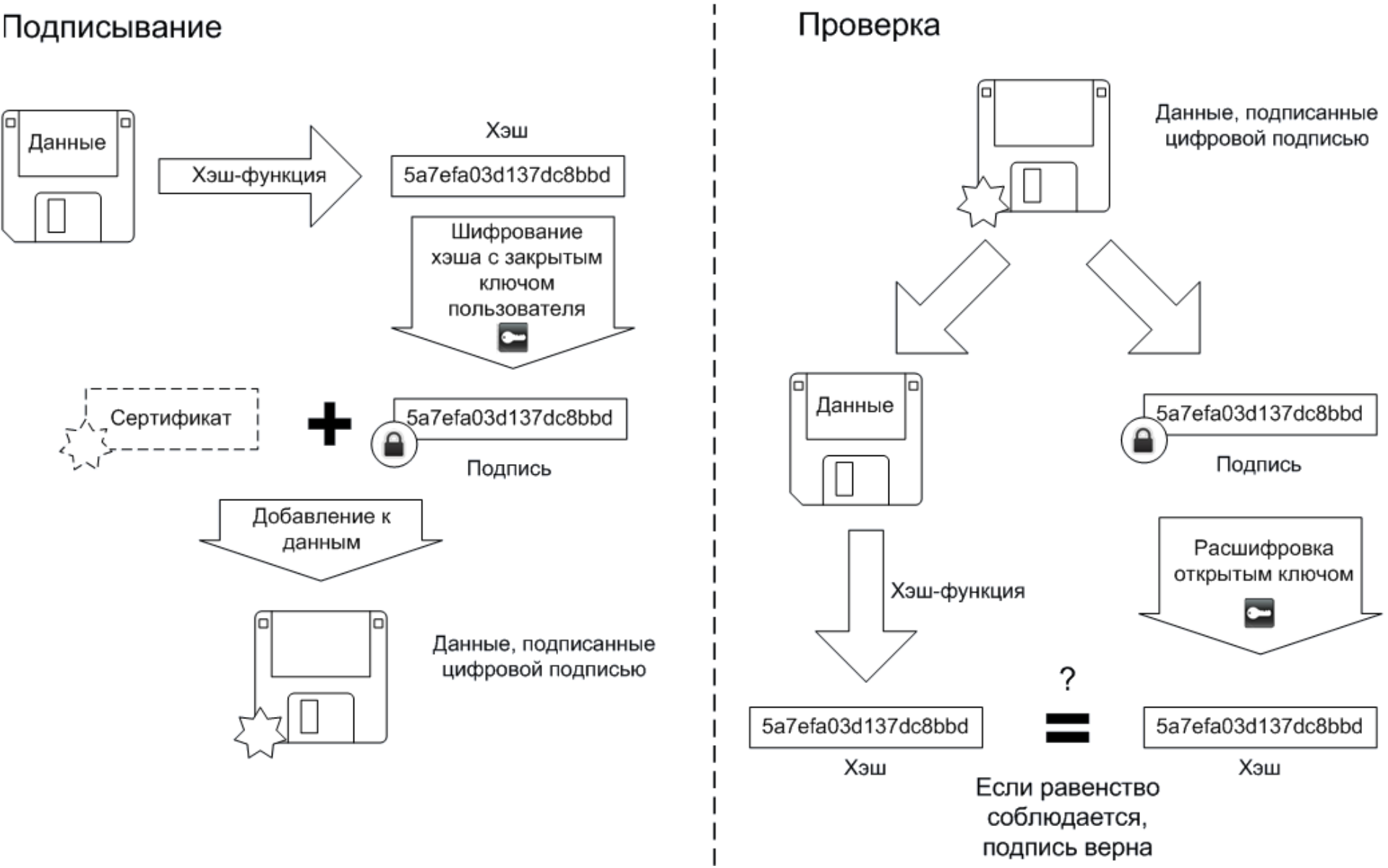
Представим шифруемое сообщение как последовательность чисел в диапазоне от 0 до 32. Буква A =1, B=2, C=3.

Теперь зашифруем сообщение, используя открытый ключ {7,33}

C1 = (3^7) mod 33 = 2187 mod 33 = 9;
C2 = (1^7) mod 33 = 1 mod 33 = 1;
C3 = (2^7) mod 33 = 128 mod 33 = 29;
Теперь расшифруем данные, используя закрытый ключ {3,33}.

M1=(9^3) mod 33 =729 mod 33 = 3(C);
M2=(1^3) mod 33 =1 mod 33 = 1(A);
M3=(29^3) mod 33 = 24389 mod 33 = 2(B);

Цифровая подпись

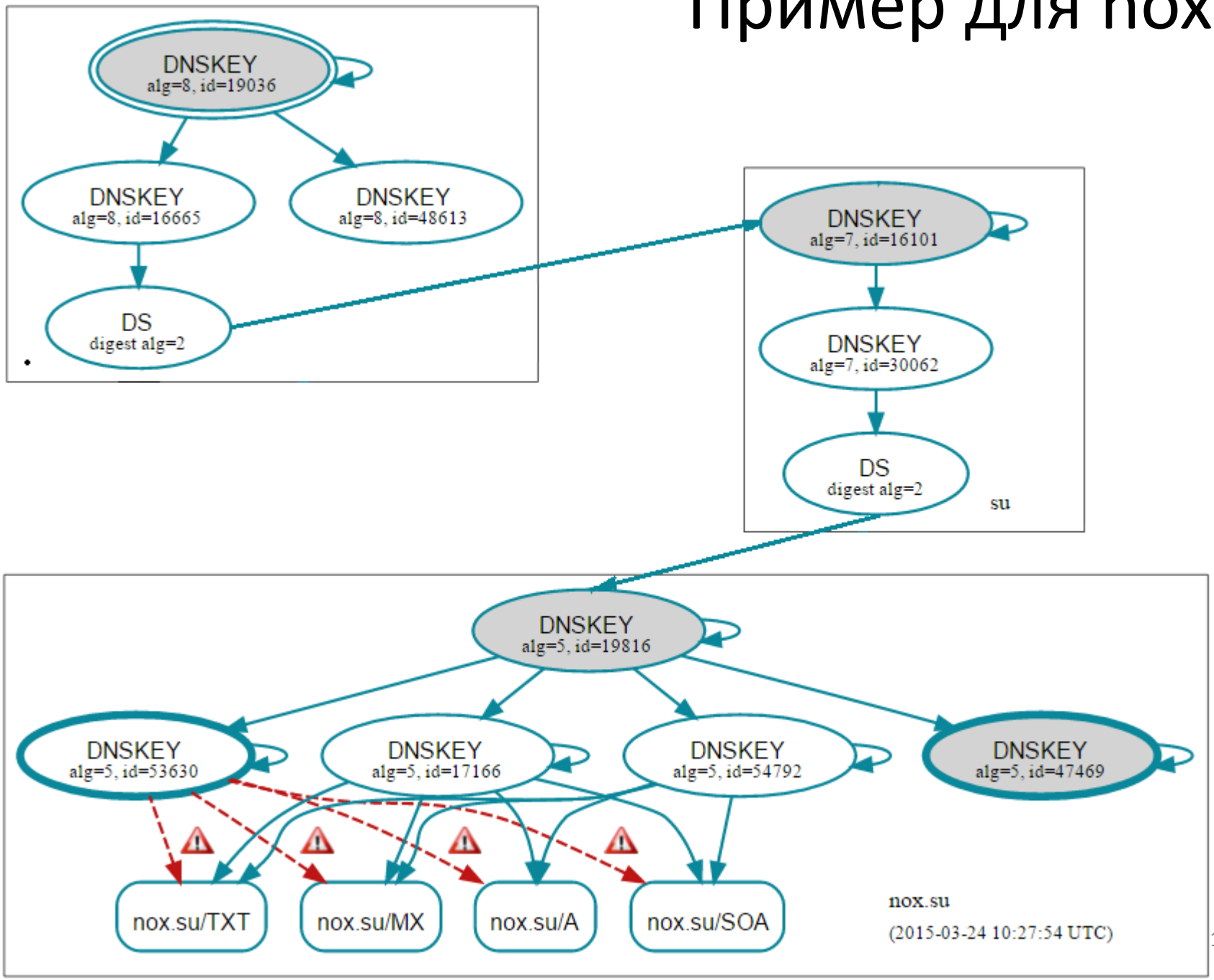


Domain Name System Security Extensions

DNSSEC – набор расширений протокола DNS, позволяющих минимизировать атаки, связанные с подменой DNS-адреса при разрешении доменных имен.

Направлен на предоставление DNS-клиентам аутентичных ответов на DNS-запросы (или аутентичную информацию о факте отсутствия данных) и обеспечение их целостности.

Пример для nox.su



Ресурсные записи DNSSEC

DS (Delegation Signer) – для идентификации ключа делегированной зоны. Содержит значение хеш-функции, открытого ключа, который должен находиться в одной из DNSKEY-записей делегируемой зоны. Размещается в делегирующей зоне, при условии наличия NS-записей для зоны делегируемой.

DNSKEY (DNS Key) – для публикации криптографических ключей в зоне. Содержит тип ключа, используемый алгоритм, сам ключ.

RRSIG (Signature RR) – для подписания других ресурсных записей. Содержит значения подписей, сгенерированных для наборов ресурсных записей зоны.
Валидность той или иной подписи может быть проверена при помощи ключей, размещённых в соответствующих DNSKEY-записях.

DNSKEY: конкретный пример

su 345600 DNSKEY 256 3 7
AwEAAfWZHDRorjygm9vbdoAyMWttyXigyCwif0STSxjeaUwKbl1SwI8E06pqyPXi
JRapdqNPPwizTWF4/LamaFNf6ZN8LSzgUe+t3vWOmG6oYps4dGBsZTasznHEP1
0IFBTuyt7aqffjW9Oza6wXreXCsqXAnrGi 6kpPs+G8oZgDQMXz ; key tag = 30062

su 345600 DNSKEY 257 3 7
AwEAAakz9eb3Pqr8hVaCowuxLWNaZlEDKvF6t8nKyN77cVVKGOm+NZ5fD/dXi4
LQtTXwS1yytFnQcRH6tMRLYS1no1Da65lO5yAod/FXMlz6M6GpWMoPY1EOGtl
C//31Eo1RfHFLzkK9UHRGJF3xs5KDmGpBsNMXd8zcLJw6T2PEjCqJueNWuTn5tp
1n6/xaKVNQhUcYx9pBFLdaZQ7aW+t6cDlm2IMn7KsOvejpX35Z7WW0TSXWDq
n1MbWAg8IAcDlF7NGBnfqRWhbjBr7Ew3iGCTt2nTiNdFGZ8oO9uSyqWhbpQJ0v
T4rl9JltbKaB6/Q1A3WH1vivI9P5uCVxxcMXnOc= ; key tag = 16101

Тип протокола = 3, всегда 3 для DNSSEC

Код алгоритма = 5, соответствует RSA с использованием SHA1

Ресурсы Интернета для DNSSEC

Анализ зон и построение схем: http://dnsviz.net

Анализ зон: http://dnssec-debugger.verisignlabs.com/

Статистика внедрение DNSSEC в домене RU:
http://stat.nic.ru/reports/whist-ru/dnssec.html

Интернациональные доменные имена

IDN (Internationalized Domain Names) – доменные имена, которые содержат символы национальных алфавитов.

президент.рф

.مصر

Для поддержки IDN достаточно, чтобы их понимал браузер.

Punycode – стандартизированный метод преобразования последовательностей Unicode-символов в ACE-последовательности (ASCII Compatible Encoding).

Преобразованные имена должны начинаться с префикса: xn--
http://xn--80acd.com – IDN в Punycode-представлении,
http://80acd.com – обычное доменное имя.

Примеры Punycode преобразования

Последовательность символов	**Кодировка**
abcdef	abcdef
abæcdöef	abcdef-qua4k
schön	schn-7qa
ยจฆฟคฎข	22cdfh1b8fsa
☺	74h
правда	80aafi6cg