Криптография - 3

Виталий Павленко, «Интеллектуал»

План лекции

- Повторение
- Trusted timestamping
- Электронный чек

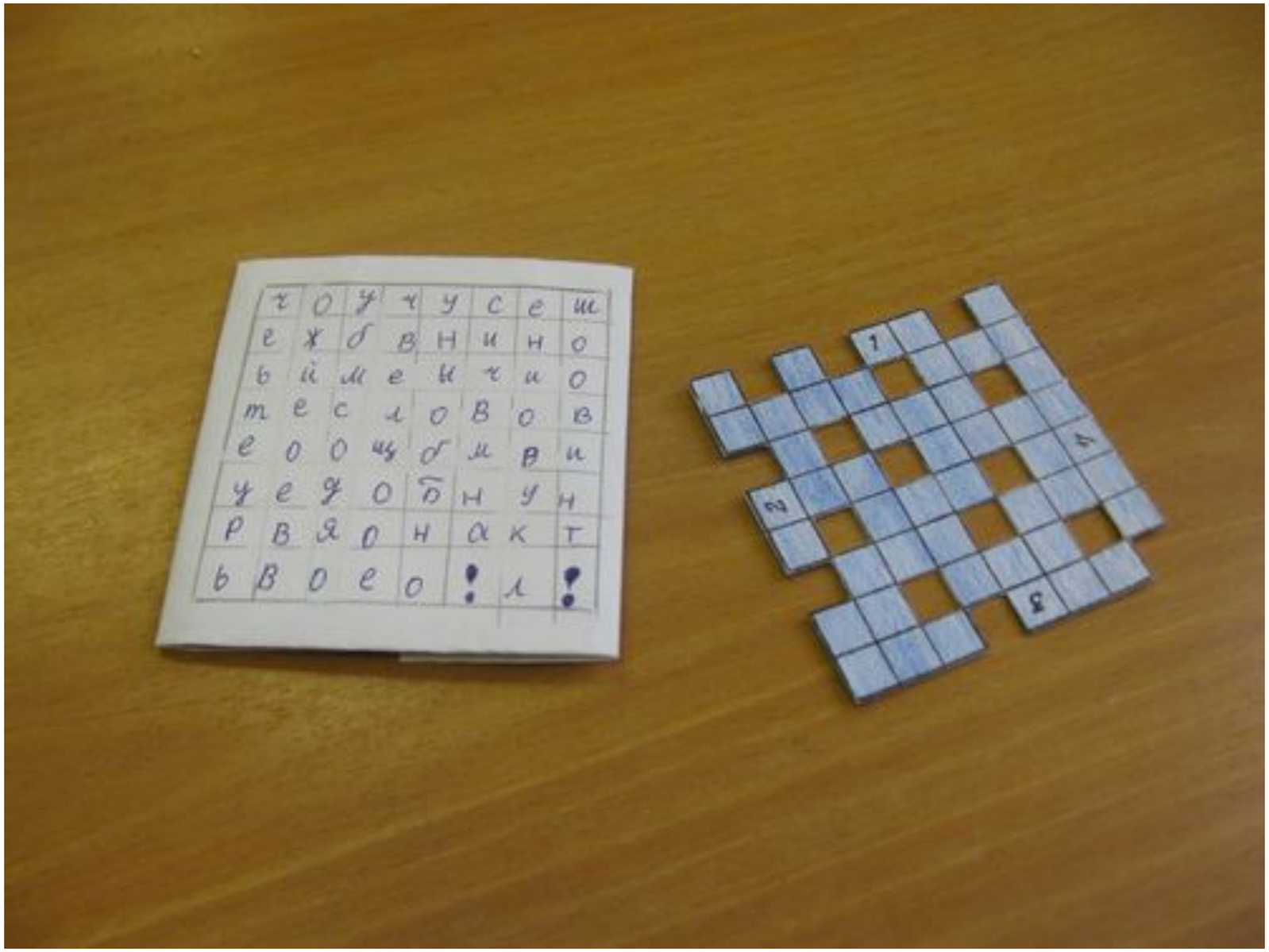
Повторяем симметричное шифрование

- Правило рубрики: на каждый вопрос отвечает человек, который пока что отвечал меньше остальных
- Что такое шифр Виженера?
- Что такое SP-сеть?
- Используются ли шифры вроде AES на практике?

Что это?

к	н	с	а	а	я	с	о
м	ж	ы	к	п	д	е	т
р	о	е	ы	щ	м	д	й
о	е	с	а	ж	в	а	е
с	л	т	т	м	и	т	р
с	з	е	е	п	а	т	с
и	п	а	е	м	е	с	р
ь	б	с	а	я	я	н	й

Решетка Кардано



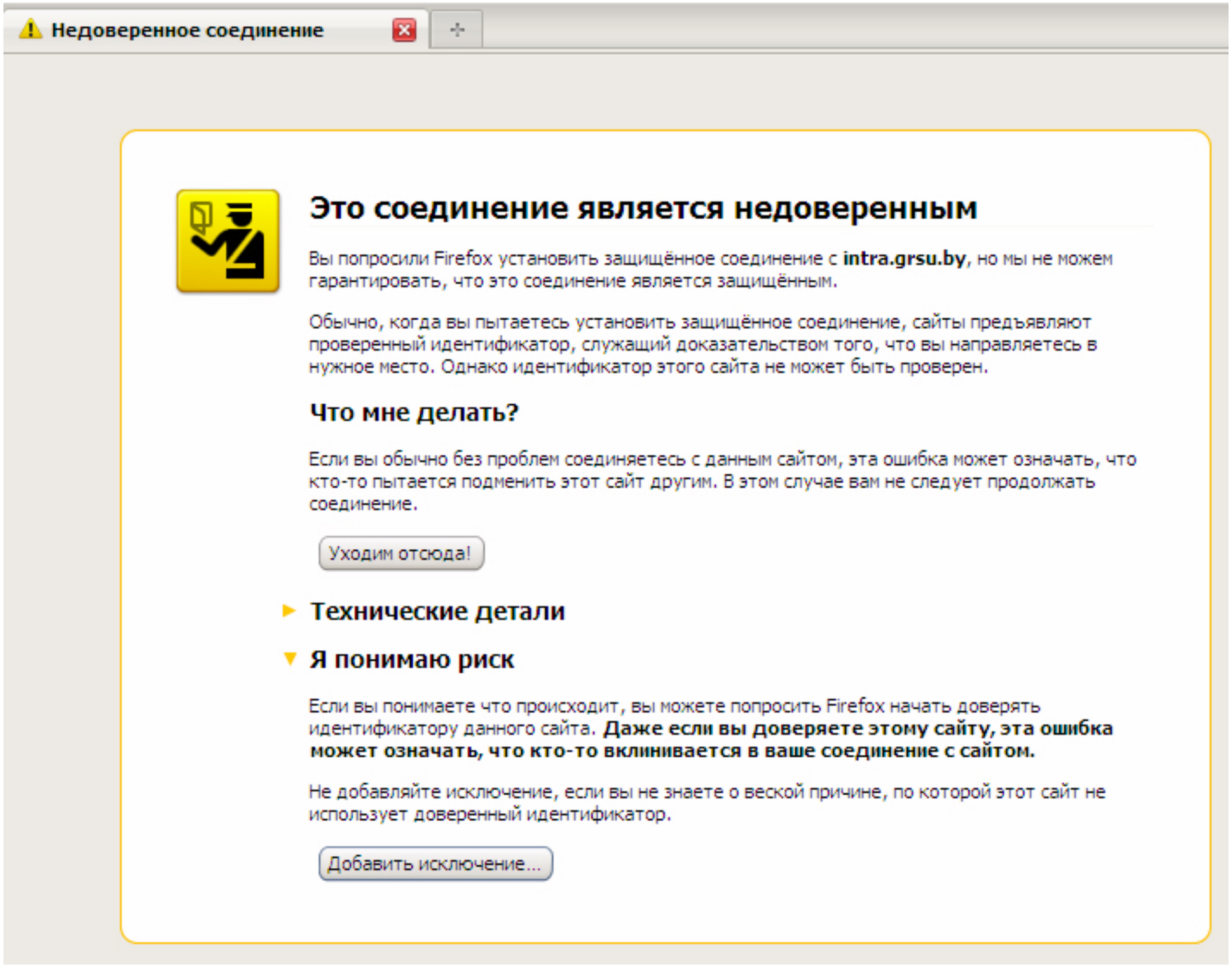
Повторяем хеши

- Какими свойствами должна обладать функция h(x), чтобы человечество её использовало в качестве хеш-функции?
- Как устроена хеш-функция SHA-1?
- Какие атаки на хеш-функции известны?
- Как и зачем люди солят хеши?
- Догадайтесь, какая атака на SHA-3 до сих пор не была проведена ни одним человеком?

Повторяем публичный ключ

- Как работает разделению секрета по методу Диффи-Хеллмана?
- А можно ничего не брать по модулю?
- Как быстро посчитать g^b (mod p), если b большое?

Что это значит?



Trusted timestamping

Как подписать документ текущей датой?

Например, мы хотим уметь доказывать,
что 2 апреля эта презентация уже существовала

Протокол

- Алиса хочет переслать Бобу документ с отметкой времени
- Алиса пересылает документ T в центр подписи
- Центр подписи получает документ T, смотрит на текущее время t и зашифровывает пару (T, t) своим закрытым ключом

Проблемы протокола

- Алиса вынуждена разглашать документ T центру подписи, а он может быть секретным
- Где гарантия, что Алиса не вступила в сговор с центром подписи? Как центр подписи может доказывать свою безупречную репутацию?
- Предлагайте улучшения к протоколу

Электронный чек

Зачем нужен электронный чек?

- Обычные платежи: есть банк, который хранит наши деньги. Для каждой транзакции банк знает отправителя и получателя

- Хотим, чтобы Алиса могла передать деньги Бобу, и Боб как получатель не стал известен банку

- Выпишем Бобу анонимный чек, подписанный банком. По этому чеку Боб обналичит деньги

- Чек не должен содержать имени Алисы, но должен содержать подпись банка

Протокол 1

Alice creates a message M="This is worth \$20, date, time, S". Here S is a long random serial number used to distinguish this bill from others. She creates a random r with $\gcd(r, n_B) = 1$. Alice sends $M' := Mr^{e_B} \bmod n_B$ to the bank and tells them to deduct \$20 from her account. The bank signs blindly as above and sends Alice $M'' := (M')^{d_B} \bmod n_B$. Alice computes $M''' := M''r^{-1} \equiv M^{d_B} (\bmod n_B)$. Alice computes $(M''')^{e_B} \equiv (M^{d_B})^{e_B} (\bmod n_B)$ and confirms it equals M. Alice sends M, M''' to Carol. Carol computes $(M''')^{e_B} \bmod n_B$ and confirms it equals M. Carol reads "This is worth \$20 ...". Carol sends M''' to the Bank. The bank computes $(M''')^{e_B} \bmod n_B = M$ and puts \$20 in Carol's account. Only then does Carol give the book to Alice.

Проблема протокола 1

Problem 1. Alice could create the message M="This is worth \$20 ..." and tell the bank to deduct \$5 from her account. Since the bank can not figure out M during the interaction with Alice, the bank can not detect the cheating.

Протокол 2

Solution 2 (preferred as it will work well with eventual full solution). Alice blinds 100 different messages M_i="This is worth \$20, date, time, S_i" for $i = 1, \ldots, 100$, each with a different r_i (S_i is the serial number). The bank randomly picks one of them and signs it and asks Alice to unblind the rest. (In homework, you will determine how to unblind.) The other 99 had better say "This is worth \$20 $\ldots, S_i$". You can increase the number 100 to make it harder for Alice to cheat.

Проблема протокола 2

Problem 2. Alice can buy another book from David for \$20 using the same $M''' = M^{d_B}$ again. The bank will notice that the serial number has been used twice, but not know that it was Alice who cheated. Putting a serial number in M that is tied to Alice will not help because then Alice loses her anonymity.

Решение существует

Подробности:

Edward Schaefer. An introduction to cryptography and cryptanalysis