АСИМЕТРИЧНО ШИФРОВАЊЕ

Шифровање јавним кључем

- Алгоритми шифровања засновани су на математичким функцијама, а не на једноставним операцијама над битима
- Шифровање је асиметрично и укључује употребу два различита кључа
- Нема неких предности у односу на конвенционално шифровање тајним кључем

Шема шифровања јавним кључем

- Отворени текст – порука на улазу
- Алгоритам за шировање – трансформише отворени текст
- Јавни и приватни кључ – то је пар кључева (један за шифровање, други за дешифровање)
- Шифрат – шифрована порука која зависи од отвореног текста и кључа
- Алгоритам за дешифровање – генерише оригинални отворен текст помоћу шифрата и одговарајућег кључа

Основни кораци шифровања јавним кључем

- Сваки корисник генерише пар кључева који ће се користити за шифровање и дешифровање порука
- Сваки корисник ставља један од два кључа у јавни регистар (јавни кључ). Други придружени кључ се чува у тајности
- Порука се шифрује помоћу јавног кључа примаоца, а дешифрује помоћу тајног кључа који има само прималац поруке

Појам система са јавним кључем

- Ради увођења шифарских система са јавним кључевима, дефинише се једносмерна функција (One-Way Function, OWF) $f : M \to X$ таква да је “лако" израчунати $f(m) = c$ док је “тешко" израчунати $f^{-1}(c) = m$
- За једносмерну функцију се каже да поседује замку (Trapdoor One-Way Function, TOF) ако се може лако инвертовати под условом да се познаје додатна информација. Таква додатна информација се назива замка.

- Ради имплементације шифарског система са јавним кључем, ако је дата фамилија једносмерних функција са замком, сваки корисник U изабере на случајан начин кључ u из K и публикује E_u помоћу кога може да се израчуна f_u
- E_u је његов јавни кључ, док је замка $t(u)$ неопходна за инвертовање f_u његов тајни кључ.

- Ако корисник *A* жели да пошаље поруку *m* другом кориснику *B*, пронађе у регистру јавних кључева јавни кључ корисника *B*, E_b и пошаље $f_b(m) = c$ кориснику *B*.

- Како једино *B* може да инвертује f_b једино он може да реконструише поруку *m*

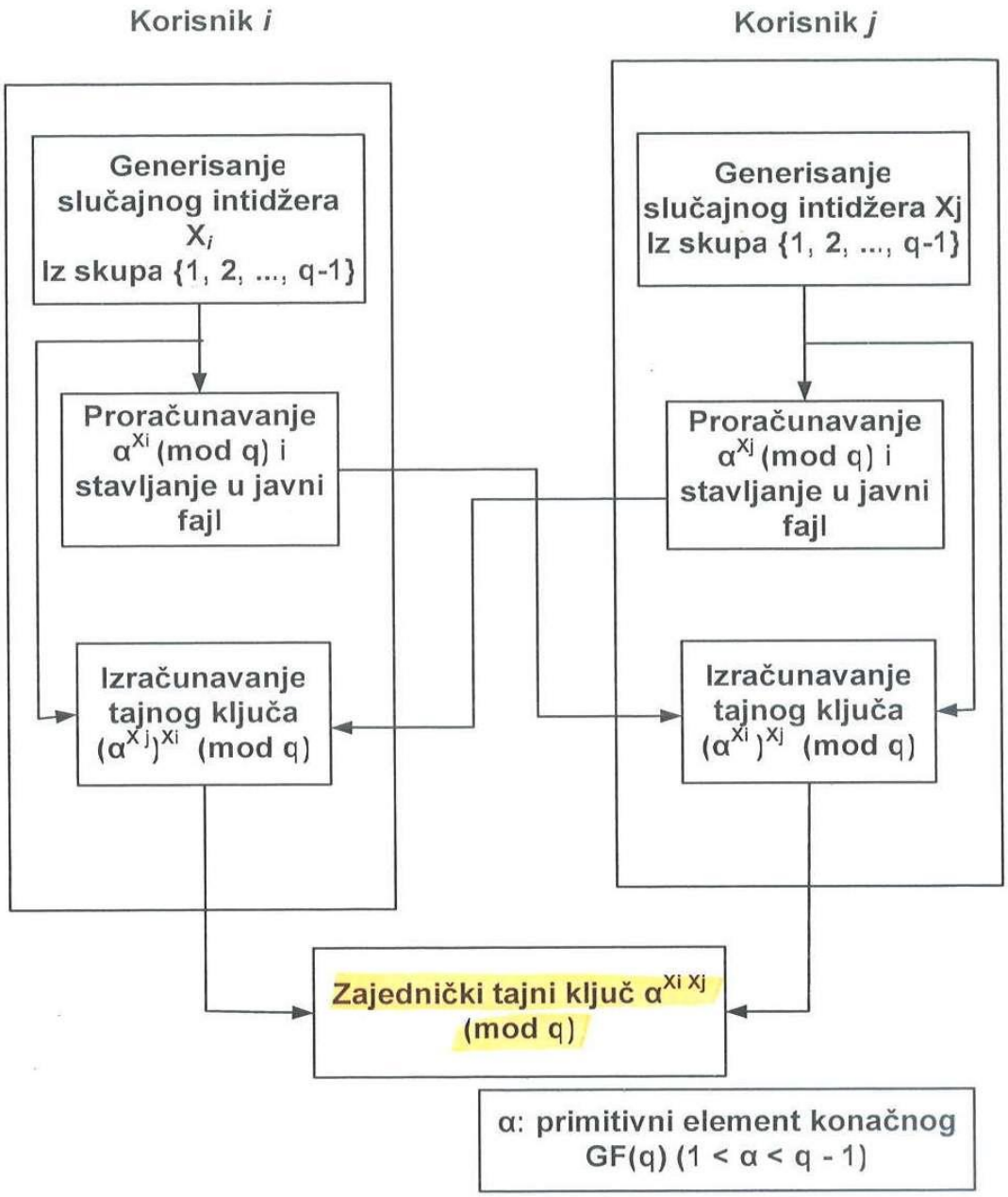
$$f_b^{-1}(c) = f_b^{-1}(f_b(m)) = m$$

- Проблем са системима са јавним кључевима састоји се у томе што није доказана егзистенција ни једносмерних функција ни једносмерних функција са замком.
- Упркос томе, постоје две функције које се сматрају кандидатима за функције са поменутим својствима.
  - Производ целих бројева, чија инверзна функција је факторизација добијеног броја,
  - Дискретна експоненцијација, чија је инверзна функција дискретни логаритам.
- Ове две функције су лаке за израчунавање, док се верује да то није случај са њиховим инверзним функцијама.

- На пример, ако је дат број n, верује се да је тешко одредити његову декомпозицију на просте факторе и, са друге стране, ако су дати бројеви a и b, верује се да је тешко израчунати x тако да је $a^x = b$
- На тај начин, сигурност система са јавним кључевима који се данас користе у пракси зависи од броја операција потребног да би се инвертовале поменуте функције и још увек није доказано да не постоји алгоритам за њихово лако инвертовање.

- Појам система са јавним кључевима увели су Diffie и Hellman 1976. године.
- Први такав систем који су они дефинисали био је протокол, познат под именом размена кључева Diffie-Hellman.
- Два корисника, *A* и *B*, изаберу јавно коначну мултипликативну групу, *G*, реда *n* и један њен елемент $\alpha \in G$
- *A* генерише случајан број *a*, израчуна α^a у *G* и пошаље овај елемент кориснику *B*.

- *B* генерише случајан број *b*, израчуна α^b у *G* и пошаље овај елемент кориснику *A*.
- *A* прими α^b и израчуна $\left(\alpha^b\right)^a$ у *G* .
- *B* прими α^a и израчуна $\left(\alpha^a\right)^b$ у *G*.
- На тај начин, *A* и *B* поседују заједнички тајни елемент из групе *G* - α^{ab}
- Криптоаналитичар *S* може да познаје *G*, *n*, α^a α^b и треба да израчуна елемент α^{ab}
- Али проблем је у томе што је тај прорачун еквивалентан израчунавању дискретног логаритма. Зато се верује да је “тежак".



Slika 4.2 – Difi-Helman-ova razmena eksponencijalnog ključa

Пример

- Нека је p прост број 53. Претпоставимо да је $G = Z_{53}^*$ и нека је $\alpha = 2$ један од њених генератора. Протокол Diffie-Hellman је следећи низ операција:
- A бира $a = 29$ израчунава $\alpha^a = 2^{29} \equiv 45 \pmod{53}$ и шаље 45 кориснику B.

- *B* бира $b = 19$ израчунава $\alpha^b = 2^{19} \equiv 12 \pmod{53}$ и шаље 12 кориснику *A*.
- *A* прима 12 и израчунава $12^{29} \equiv 21 \pmod{53}$
- *B* прима 45 и израчунава $45^{19} \equiv 21 \pmod{53}$
- Приватни кључ или тајна информација коју сада деле *A* и *B* је 21.

- Криптоаналитичар *S* познаје Z_{53}^{*} , 2, 45 і 12, али не може да реконструише да је информација коју деле *A* и *B* једнака 21 зато што мора да израчуна дискретни логаритам да би то одредио.

Rivest-Shamir-Adleman (RSA) алгоритам

- 1983. Године Rivest, Shamir и Adleman су патентирали шифарски систем са јавним кључевима познат под именом RSA (иницијли аутора) алгоритам.
- Сваки корисник U изабере два проста броја (данас се препоручује да ти бројеви имају више од 200 цифара) p и q и рачуна $n = p \cdot q$ То значи да је група коју користи корисник U Z_n^*

Ред те групе је:

$$\phi(n) = \phi(p \cdot q) = (p-1)(q-1)$$

Кориснику U је лако да израчуна овај ред, пошто зна p и q.

Затим U изабере позитиван број e,

$$1 \leq e < \phi(n)$$

такав да је узајамно прост са редом групе, тј. такав да је НЗД $(e, \phi(n)) = 1$

- Помоћу генерализованог Еуклидовог алгоритма корисник U израчуна инверзни елемент од e у $Z_{\phi(n)}$, d. Значи

$$e \cdot d \equiv 1 \left(\mathrm{mod}\, \phi\left(n\right)\right)$$

при чему је $1 \leq d < \phi\left(n\right)$

- Јавни кључ корисника U је пар $\left(n, e\right)$ док је његов приватни кључ број d.

- Бројеви p, q и $\phi\left(n\right)$ такође морају да се држе у тајности.

- Ако корисник А жели да пошаље поруку m из M другом кориснику В, користи јавни кључ корисника В, (n_b, e_b) да би израчунао вредност $m^{e_b} \pmod{n_b} = c$ коју шаље кориснику В.
- Да би реконструисао поруку, В рачуна

$$c^{d_b} = \left(m^{e_b}\right)^{d_b} = m^{e_b d_b} \equiv m \pmod{n_b}$$

Пример:

- Размотримо кодирање алфабета које трансформише слова A до Z у бројеве 0 до 25 (користићемо енглески алфабет). Желимо да пошаљемо поруку кориснику B.
- Корисник B бира два проста броја: $p_b = 281$ и $q_b = 167$, рачуна $n_b = 281 \cdot 167 = 46927$ што значи да ради са групом Z^*_{46927}

- Ред ове групе је:
$$\phi(46927) = 280 \cdot 166 = 46480$$
- *B* бира број $e_b = 39423$ и верификује да је НЗД $(39423, 46480) = 1$
- Затим одређује инверзни елемент од 39423 по модулу 46480. Овај број је
$$d_b = 26767$$
- Значи јавни кључ корисника *B* је:
$$(n_b, e_b) = (46927, 39423)$$

док остале вредности држи у тајности.

- Да бисмо послали поруку кориснику *B*, морамо да одредимо на првом месту њену дужину.
- Имаћемо у виду да се кодовање слова алфабета врши у бази 26.
- Како порука мора да буде елемент групе са којом радимо, њена дужина не може да пређе вредност $n = 46927$
- Зато ако се има у виду да је

$$26^3 = 17576 < n < 456976 = 26^4$$

порука може да има највише три слова.

- Ако желимо да пошаљемо дужу поруку, морамо да је поделимо на групе од по три слова.
- У пракси је дужина поруке много већа, пошто је n број са много више цифара.

- Ако, на пример, желимо да пошаљемо кориснику *B* поруку *m*="YES", процедура је следећа:
- Претпостаимо да смо корисник *A* чији је јавни кључ $(n_a, e_a) = (155011, 2347)$ и чији је приватни кључ $d_a = 151267$ при чему је

  $p_a = 409 \quad q_a = 379 \quad \phi(n_a) = 154224$

- Да бисмо послали поруку *m*, морамо да је кодујемо, тј. да је изразимо у бази 26 тако да буде елемент групе која се користи, што значи да припада Z^*_{46927}

$$YES = Y \cdot 26^2 + E \cdot 26 + S = 24 \cdot 26^2 + 4 \cdot 26 + 18 = 16346 = m$$

- Сада шифрујемо m јавним кључем корисника B:

$$c = m^{e_b} \pmod{n_b} = 16346^{39423} \pmod{46927} = 21166$$

- Декодујемо шифровану поруку:

$$c = 21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2 = BFIC$$

- Значи, кориснику B се шаље следећи текст: "BFIC".

- Да би *B* могао да реконструише поруку, мора да кодује примљене податке у бази 26, а затим да реализује следеће операције:

$$BFIC = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2 = 21166 = c$$

- Сада може да реконструише *m*

$$m = c^{d_b} \left(\mathrm{mod}\, n_b \right) = 21166^{\,26767} \left(\mathrm{mod}\, 46927 \right) = 16346$$

m се декодује и добија се оригинални текст

$$m = 16346 = 24 \cdot 26^2 + 4 \cdot 26 + 18 = YES$$

- У пракси, ради смањења сложености операција у шифарском систему RSA, обично се бира мали јавни кључ, тако да се порука може послати на најбржи могући начин.
- Многи корисници користе унутар својих јавних кључева исти експонент (најчешће коришћени експоненти су 3 и $2^{16}+1$).
- Ова чињеница не компромитује безбедност шифарског система и омогућава да шифровање порука буде много брже него дешифровање.

- Са алгоритамске тачке гледишта, ако је k број бита модула n, за извршење операција са јавним кључем потребно је $O\left(k^3\right)$ корака, а за генерисање кључева потребно је $O\left(k^4\right)$ корака.
- Због тога је у практичној реализацији софтвера шифарски систем са тајним кључем DES најмање 100 пута бржи од RSA, а у практичној реализацији хардвера DES је између 1000 и 10000 пута бржи од RSA.
- Ипак, шифарски систем RSA се користи у пракси за потребе технологије дигиталног потписа.

Primer zadatka:

- Parametri RSA algoritma.
- Operacije sa privatnim i javnim ključem.
- Ukoliko su vrednosti parametara u RSA algoritmu:
- p=17,
- q=11,
- javni eksponent e=3.
- Odrediti vrednost parametra n (modulus) i privatnog eksponenta d?

Rešenje:

- a) Parametri RSA algoritma su:
  - p, q, dva prosta broja (privatni, generisani).
  - n=p*q (javni, izračunava se)
  - e pri čemu NZD((p-1)*(q-1),e)=1 (javni, odabira se)
  - d *e≡1mod (p-1)*(q-1), (privatni, izračunava se)

Rešenje:

- Operacije sa privatnim i javnim ključem.
  - Javni ključ KU={e,n}
  - Privatni ključ KR={d}
  - važeće su sledeće relacije za poruke otvorenog teksta M za poruke šifrata C, i celobrojne vrednosti e i d
    - operacija sa javnim ključem:

$$C = M^e \bmod n$$

    - operacija sa privatnim ključem:

$$M = C^d \bmod n = M^{ed} \bmod n$$

Rešenje:

c) Modulus n = p*q => n=17*11=187

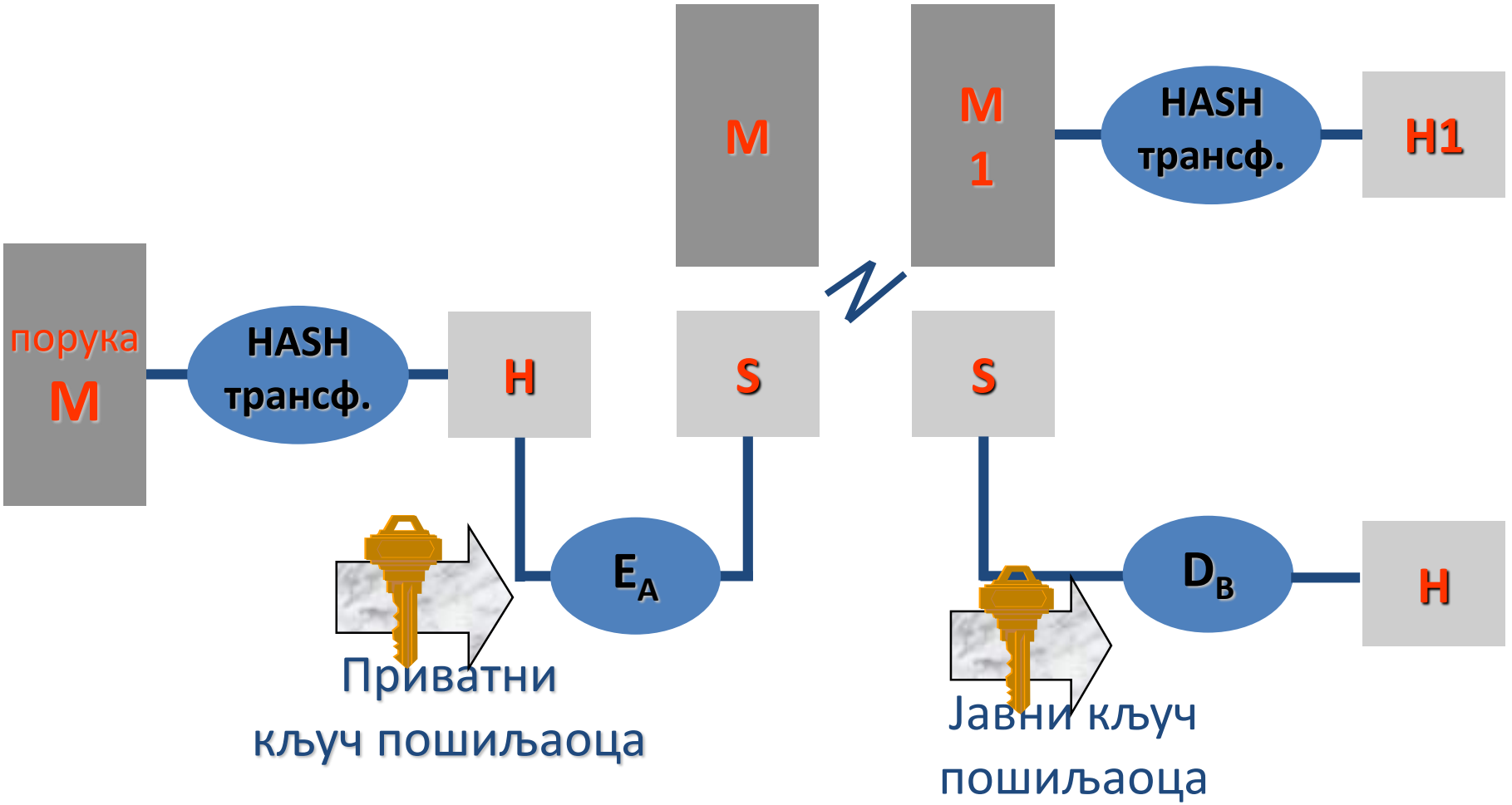
tj.
3 * d mod (17-1)*(11-1) = 1,
3 * d mod 160 = 1

Niz brojeva *x* za koje je *x* mod 160 =1 je
161 mod 160 =1,
321 mod 160 =1,
481 mod 160 =1,
641 mod 160 =1,
801 mod 160 =1,
.
.
.
stoga proizvod 3**d* je najmanji broj *x* koji zadovoljava da je 3**d* = *x* gde je *d* celobrojna pozitivna vrednost tj.
Prvi kandidat 3**d* = 161 => ne postoji ceo broj *d* koji zadovoljava jednačinu
Sledeći kandidat 3**d* = 321 => *d* = 321/3 = 107.

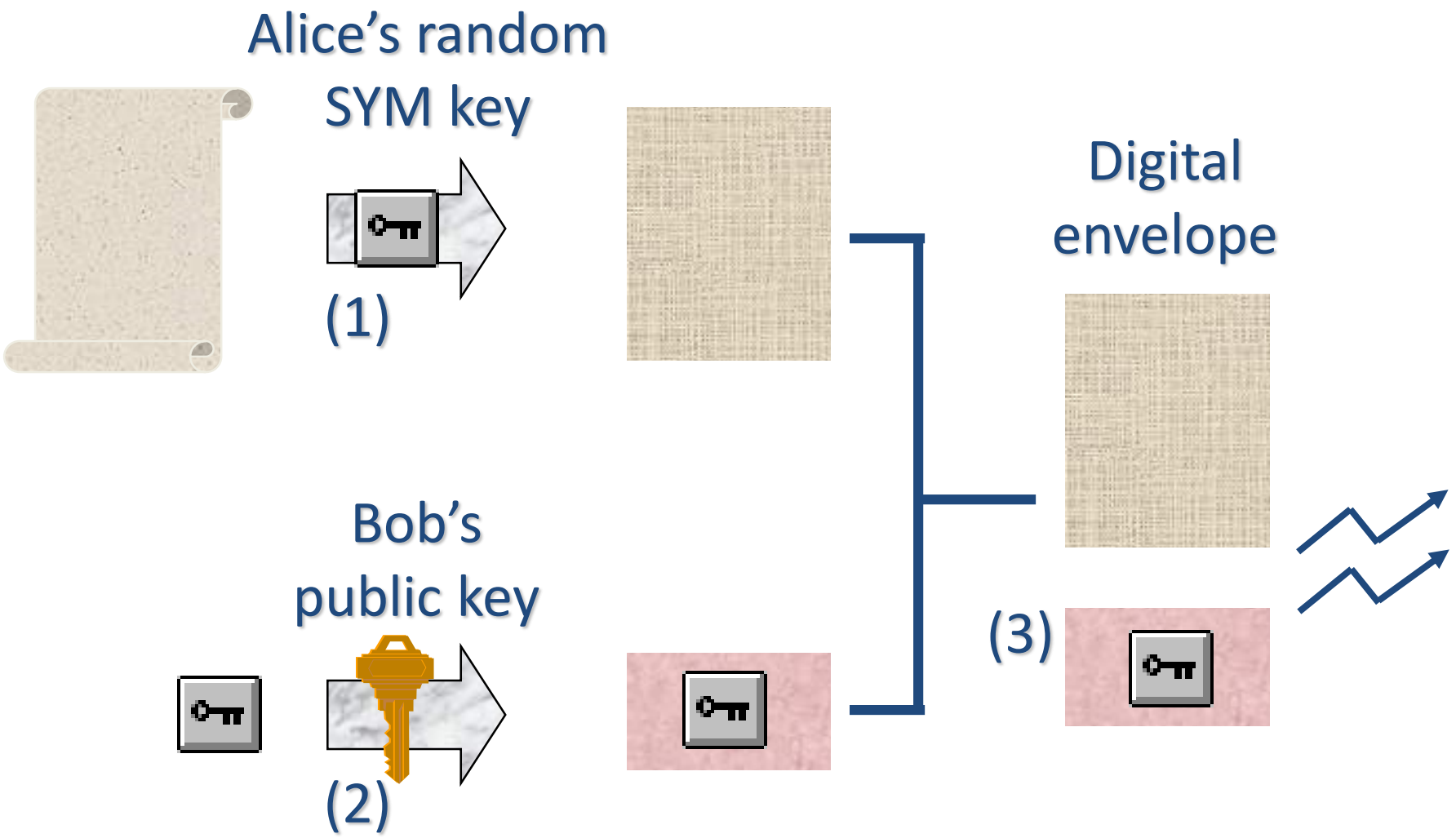
Дигитални потписи

- Користи се шифровање јавним кључем, али сада пошиљалац користи приватни кључ
- Прималац може да дешифрује поруку само јавним кључем пошиљаоца, што доказује да је порука његова
- Због ефикасности шифрује се мали блок бита који је функција целог документа
- Остатак поруке је отворен и подложан прислушкивању
- SHA-1 може да служи као дигитални потпис

Дигитални потпис



Дигитална енвелопа



Digital Envelope (cont'd)